IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re Dealer Management Systems Antitrust Litigation, MDL 2817	No. 1:18-CV-864
This document relates to:	Hon. Robert M. Dow, Jr.
Authenticom, Inc. v. CDK Global, LLC et al., Case No. 1:18-cv-868 (N.D. Ill.)	Magistrate Judge Jeffrey T. Gilbert

DEFENDANT THE REYNOLDS AND REYNOLDS COMPANY'S ANSWER TO ORIGINAL COMPLAINT, AFFIRMATIVE DEFENSES, AND COUNTERCLAIMS

Defendant The Reynolds and Reynolds Company ("Reynolds"), files this answer, affirmative defenses, and counterclaims to Authenticom, Inc.'s ("Authenticom") Complaint. Except as expressly admitted herein, Reynolds denies each and every allegation contained in the Complaint, including but not limited to any allegations contained in the preamble, headings, subheadings, or footnotes of the Complaint. Reynolds reserves the right to amend and/or supplement its answer, affirmative defenses, and counterclaims.

REYNOLDS'S ANSWER TO COMPLAINT

Reynolds responds to the each of the paragraphs of the Complaint as follows:

INTRODUCTION

1. Denied.

2. Admitted that the DMS performs system functions important to the automotive industry. Admitted that, in the course of their operations, automobile dealerships often generate important data using proprietary data of others, including vehicle and parts inventory (which often includes data belonging to car manufacturers or Original Equipment Manufacturers (OEMs), customer name and contact information, completed and pending sales, vehicle financing and

insurance information). Admitted that some dealers have in the past set up login credentials for certain vendors so that they can access data in the DMS, but denied that dealers can validly authorize third parties to access Reynolds's DMS; denied that such actions were permitted by Reynolds contracts or security protocols; and denied that such efforts were reliably successful during the relevant time period. Admitted that Authenticom reformats the data that it extracts from DMS systems and that it provides data to third parties for a fee. However, Reynolds is unable to determine to what extent Authenticom reformats the data into a "usable form," and therefore denies same. As to all remaining allegations of this paragraph of the Complaint, denied.

3. Admitted that Dealer Management Systems are referred to as "DMS" and that most new vehicle franchised dealerships and many used-car and independent dealerships rely on a DMS to manage and operate their dealerships. Admitted that the DMS contains databases where system data is stored; denied that "dealers enter their data into a database within the DMS." In addition, a very small percentage of new vehicle franchised dealerships operate without a DMS. Admitted that CDK and Reynolds are currently the two largest providers of DMS products to new vehicle franchised dealerships in the United States (without conceding that the United States or new vehicle franchised dealerships are the relevant market at issue in this case). As to all remaining allegations of this paragraph of the Complaint, denied.

4. Denied as to Reynolds.

5. Admitted that Tom Schwartz of Reynolds made the statement attributed to Reynolds, but denied as to Plaintiff's interpretation of this statement, which is taken grossly out of context. Upon information and belief, admitted that CDK made the statement attributed to it. As to all remaining allegations in this paragraph of the Complaint, denied.

6. Admitted that the quoted language appears in an industry publication and was attributed to Steven Anenen. Reynolds denies, however, that Authenticom has fairly characterized the article, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

7. Admitted that the quoted language, taken out of context, is attributable to Mr. Brockman. Reynolds denies, however, that Authenticom has fairly characterized the article, which speaks for itself. Admitted that Reynolds unilaterally tried to block (and largely succeeded in blocking) CDK and its subsidiaries from accessing Reynolds's DMS without authorization. Reynolds denies all other allegations of this paragraph of the Complaint.

8. To the extent this Paragraph purports to refer to Defendants' Data Exchange Agreement, Reynolds denies all characterizations of this agreement in this paragraph of the Complaint, but admits that the Data Exchange Agreement was entered into in February 2015. On information and belief, admitted that the quoted language appears in a CDK letter sent to its vendor clients on or about March 2, 2015. That letter speaks for itself. In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and Authenticom elected not to replead it. As to all remaining allegations in this paragraph of the Complaint, denied.

9. Denied. In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and Authenticom elected not to replead it.

10. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint as it relates to CDK, and therefore denies same.

11. Admitted that Reynolds has prohibited dealers from providing access to Reynolds's proprietary DMS to third parties, but denied that such prohibition was made in furtherance of or pursuant to any agreement with CDK, that such prohibition barred dealers from providing access to their data, and that such prohibition barred dealers from doing business with Authenticom (or other putative "integrators"). Reynolds's DMS licensing agreements with dealers have included such restrictions since long before Data Exchange Agreement. The Court has previously rejected the dealer contract exclusive dealing theory, and Authenticom has elected not to replead it. As to all remaining allegations of this paragraph of the Complaint, denied.

12. Denied as to Reynolds. As to CDK, Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

13. Admitted that the quotations were made by then-President Obama. As to the number of dealers and vendors purportedly served by Authenticom, Reynolds lacks knowledge or information sufficient to form a belief about the truth of those allegations, and therefore denies same. As to the remaining allegations of this paragraph of the Complaint, denied.

14. Denied.

15. As to Authenticom's and CDK's average charges to vendors, Reynolds lacks knowledge or information sufficient to form a belief about the truth of those allegations, and therefore denies same. As to the remaining allegations of this paragraph of the Complaint, denied.

16. Denied.

17. Denied. In addition, the Court has previously rejected the dealer contract exclusive dealing theory, and Authenticom has elected not to replead it.

18. Admitted that Authenticom alleges federal antitrust and Wisconsin tort violations and seeks to recover damages and an injunction; denied that Reynolds has violated any federal antitrust laws or Wisconsin tort laws, that Authenticom is entitled to any damages, and that Authenticom is entitled to an injunction. Reynolds denies all other allegations of this paragraph of the Complaint. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it; further, the Seventh Circuit has previously ruled that certain of the requested injunctions are improper.

PARTIES

19. Upon information and belief, admitted.

20. Upon information and belief, admitted.

21. Admitted that Reynolds is an Ohio corporation with its corporate headquarters and principal place of business at One Reynolds Way, Kettering, Ohio 45430. Admitted that Reynolds provides DMS products and services to automobile dealerships in the United States (among other countries), including Wisconsin. Reynolds admits it was publicly traded before 2006. Reynolds denies all other allegations of this paragraph of the Complaint.

JURISDICTION AND VENUE

22. Admitted that Plaintiff purports to bring this action under Sections 1 and 2 of the Sherman Act, 15 U.S.C. §§ 1 and 2; Sections 4 and 16 of the Clayton Act, 15 U.S.C. §§ 15 and 26; and Wisconsin state law. Denied that Reynolds has violated any of these laws.

23. Admitted.

24. Answering only as to Reynolds, it is admitted that this Court has personal jurisdiction over Reynolds; otherwise, denied.

25. Admitted that venue is proper in this District.

26. Denied.

FACTUAL ALLEGATIONS

I. The Relevant Product Markets

27. Denied.

A. The DMS Market

28. Admitted that Dealer Management Systems are sometimes referred to as "DMS" and that most new vehicle franchised dealerships rely on a DMS to manage and operate their dealerships. A DMS includes numerous components of software and hardware to perform its system functions. In addition, a very small percentage of new vehicle franchise dealerships operate without a DMS. Admitted that, in the course of their operations, automobile dealerships use their licensed DMS to assist in important business functions, including sales, financing, inventory management (both vehicle and parts), repair and service, accounting, payroll, human resources, marketing, and more. As to all remaining allegations of this paragraph of the Complaint, denied.

29. Denied that the DMS is equivalent to a "database" that is owned by the dealer, or otherwise. Denied that the DMS is equivalent to a database where all dealer data is stored. Denied that the dealer owns all of the data within the DMS. Otherwise, admitted.

30. Admitted that most new vehicle franchised dealerships rely on one DMS provider at a time. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

31. Denied. Reynolds's contracts vary in length and are always negotiated. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

32. Denied in part. With regard to the last sentence of this paragraph of the Complaint, while there are a variety of DMS providers and platforms with a variety of different methods and

policies for data extraction and integration, Reynolds does not deny that there are limited substitutes for DMS platforms and certain DMS services; for other DMS services there are many reasonable substitutes. Reynolds admits that the relevant DMS market for Authenticom's claims includes "retail automotive dealerships" (including, without limitation, used-car and independent dealerships). Reynolds denies all remaining allegations in this paragraph of the Complaint.

1. CDK and Reynolds Dominate the DMS Market

33. Denied in part. Admitted that CDK and Reynolds are the two largest providers of DMS products to new vehicle franchised dealerships in the United States. There are many competitive DMS providers across both franchised and independent dealers. No DMS provider is "dominant" or has market power in any relevant market. Denied as to the use of the term "control". Dealers have many choices in DMS providers in the United States. Based on best current estimates, Reynolds's current market share in the United States is less than 30% of new vehicle franchised dealerships and vastly smaller when independent dealerships are included. Depending on how one defines "independent dealerships," Reynolds either serves a very small portion of that market (*i.e.*, less than 1%), or does not serve it at all. Denied to the extent that this paragraph suggests that only franchised new car dealers, as opposed to used-car and independent dealers, are relevant to the market analysis. Admitted that Reynolds's market presence may be larger if measured by the number of vehicles sold by its dealer customers. As to CDK, Reynolds lacks sufficient information to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. As to any remaining allegations of this paragraph of the Complaint, denied.

34. Denied.

35. Admitted that there is an array of competitive DMS providers across both franchised and independent dealers. Otherwise, denied.

36. The source of these quotes is not identified; Reynolds accordingly lacks sufficient information to form a belief about the truth of allegations in this paragraph of the Complaint, and therefore denies same. Reynolds further denies the accuracy and legal relevance of the alleged characterizations.

37. As to CDK, Reynolds lack sufficient information to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. As to Reynolds, denied.

2. CDK and Reynolds Maintain Their Market Dominance by Exercising Overwhelming Leverage over Dealerships

38. Denied.

39. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint as it relates to defendant CDK, and therefore denies same. As to Reynolds, denied. Reynolds's DMS licensing agreements vary in length and are always negotiated.

40. Denied as to the first and last sentences of this paragraph of the Complaint. While switching DMS providers is not costless, those costs are nowhere close to prohibitive. Indeed, the DMS market is robustly competitive, and every year, many dealerships switch DMS providers for reasons including but not limited to price, features, performance, service, security, application availability, and third-party access policies. Reynolds denies that the quoted material is in proper context (including that one of the articles purportedly demonstrating that switching is difficult is about a dealer that did switch). Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

41. Denied in part. While the process of switching DMS providers used to take longer and can entail costs, the process of switching DMS providers now typically is much faster, and competitive DMS providers are frequently investing in new technologies and training programs to make the process easier for dealerships to switch to their DMS products. All remaining allegations of this paragraph of the Complaint are denied.

42. Admitted that Hendrick switched DMS providers for a brief period of time in 2016 and then ultimately switched back to Reynolds. Denied that Hendrick did so due to switching costs. As to the remaining allegations of this paragraph of the Complaint, denied.

43. Denied as to Reynolds.

44. Denied as to Reynolds.

45. Denied as to Reynolds. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

46. Denied.

B. The Dealer Data Integration Market

47. Admitted that the DMS enables dealers to operate and that dealers use the DMS to, among other things, process data inputted by dealers. Admitted that the data inputted to the DMS for processing (although not all by the dealer) includes vehicle and parts inventory, customer name and contact information, completed and pending sales, vehicle service and repair history, manufacturer pricing and rebate details, vehicle financing and insurance information and more. As to the remaining allegations of this paragraph of the Complaint, denied.

1. It is Essential that Application Providers Be Able to Obtain Dealer Data Stored on the DMS

48. Denied in part. Admitted that some dealers choose to use software applications or interfaces that perform certain services for the dealers, which may be in addition to or a

replacement for functions provided by the core DMS. Admitted that applications used by dealers perform functions such as vehicle inventory management, customer relationship management, electronic vehicle registration and titling, and scheduling service and repair appointments. Admitted that most dealerships use multiple, separate applications but the number of applications varies substantially by dealer. As to all other remaining allegations of this paragraph of the Complaint, denied.

49. Denied in part. Admitted that vendors that provide electronic vehicle registration and titling must be able to obtain purchaser, vehicle, and financing information about the sale of a car. Denied to the extent that this paragraph of the Complaint implies a need for access to Reynolds's proprietary DMS. While third-party application vendors typically rely on one or more data elements to provide their services, there are numerous ways that dealers can provide such data to vendors without providing the vendors or "data integrators" direct access to the DMS. Reynolds admits that dealers are required to submit vehicle registrations electronically in Wisconsin. As to all remaining allegations of this paragraph of the Complaint, denied.

50. Denied in part. Admitted that some customer relationship management ("CRM") applications utilize "bi-directional" access to some DMSs (also referred to as "write-back" access). Denied that it is a requirement for the use of any application that it have "write-back" or "push" back access to the DMS. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations of this paragraph of the Complaint, and therefore denies same.

51. Admitted that Reynolds sells a customer relationship management application, both to Reynolds's DMS customers and to dealers who use other DMS platforms. Admitted that CVR is a joint venture of CDK and Reynolds that provides electronic vehicle registration services.

Admitted that Reynolds's applications compete in certain application markets, but denied that it is "many" of them. Otherwise, denied.

52. Admitted that OEMs utilize customized interfaces to pass certain types of data to and from the Reynolds DMSs for their respective brand's dealerships. Denied that those interfaces are part of the RCI program or are relevant to this dispute. As to how OEMs interact with other DMS providers, Reynolds lacks knowledge or information sufficient to form a belief about the truth of those allegations, and therefore denies same. Otherwise, denied.

53. Denied.

2. Dealer Data Integrators Provide Dealer Data to Vendors

54. Denied in part. Admitted that there are companies that provide a service in which they extract data from a DMS, aggregate data, and deliver data to a vendor for a fee, and that such services are sometimes referred to as "data polling." Admitted that Authenticom does not provide "actual 'integration'" with the Reynolds DMS. Otherwise, denied.

55. Denied in part. Admitted that some dealers set up login credentials for certain "data integrators" like Authenticom so that they can access the DMS, but denied that dealers are authorized to do so with respect to the Reynolds DMS. Admitted that Authenticom's software generally engages in automated data scraping (or screen scraping), but as to other details of Authenticom's and others' software, Reynolds lacks knowledge or information sufficient to form a belief about the truth of those allegations, and therefore denies same. As to all remaining allegations of this paragraph of the Complaint, denied.

56. Denied in part. Admitted that certain "data integrators" use or seek to use dealership log-in credentials to infiltrate a DMS. Admitted that different DMS providers have different formats, or business rules, for the data they store and process. As to other details of

Authenticom's and others' services, Reynolds lacks knowledge or information sufficient to form a belief about the truth of those allegations, and therefore denies same.

57. Admitted that so-called "data integrators" sell data extracted from a DMS to third parties, which may include vendors selected by the dealer. As to the remaining allegations of this paragraph of the Complaint, denied.

58. Admitted that Reynolds provides the Reynolds Certified Interface ("RCI") program, which is a system of uniquely designed custom interfaces that form an integral part of the Reynolds DMS. Admitted that Reynolds does not sell a "data integration" product for non-Reynolds DMS systems. Upon information and belief, admitted that CDK owns Digital Motorworks and IntegraLink, and has a product for access to data on the CDK DMS -- the "Third Party Access" program. As to the remaining allegations of this paragraph of the Complaint related to CDK, Reynolds lacks knowledge or information sufficient to form a belief about the truth of these allegations, and therefore denies. As to the remaining allegations of the Complaint, denied.

59. Denied in part. Dealers are not authorized to allow "integrators" to pull data from or otherwise access the Reynolds DMS. Upon information and belief, Reynolds does not deny that some vendors pay Authenticom for some form of services. Reynolds lacks sufficient knowledge or information to form a belief about the truth of the allegation that dealers do not pay Authenticom, and therefore denies. As to all remaining allegations of this paragraph of the Complaint, denied.

60. Admitted that Reynolds's RCI contracts are typically three years in length. As to Authenticom's, CDK's, and other vendors' contracts, Reynolds lacks sufficient knowledge or information form a belief about the truth of these allegations, and therefore denies.

61. Denied.

62. As to the first sentence of this paragraph of the Complaint, admitted. As to all remaining allegations of this paragraph of the Complaint, denied.

63. Denied.

3. Dealers Own Their Data Stored on the DMS

64. Denied. The DMS is a licensed enterprise computer system. In addition, the DMS functionality depends on confidential and proprietary software and data, including the DMS provider's proprietary functions and data, OEM data, contracted third-party data, credit-reporting data, and other nonautomotive third parties' data.

65. Admitted in part, subject to the clarification that the first quoted language goes on to say that, "But we can't have people rooting around in a dealer's DMS. That creates a liability." Denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. As to any remaining allegations of this paragraph of the Complaint, denied.

66. Admitted that the quoted statements were attributed to CDK. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations of this paragraph of the Complaint, and therefore denies same. Denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS.

67. Denied in part. As to the allegations regarding CDK, Reynolds lacks knowledge or information sufficient to form a belief about the truth of these allegations, and therefore denies same. Admitted that the language "Reynolds recognizes that your Business Data belongs to you, and we respect and support your right to protect your Business Data" appears in Reynolds's Customer Guide, which is incorporated into its DMS contracts. Denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. As to the remaining allegations of this paragraph of the Complaint, denied.

4. Dealers Have the Right to Control Who Has Access to Their Data

68. Admitted, in part. Admitted that dealers can share data that they own subject to applicable law and contract or licensing restrictions. Denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS. As to any remaining allegations of this paragraph of the Complaint, denied.

69. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations of this paragraph of the Complaint, and therefore denies same. Denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS. As to any remaining allegations of this paragraph of the Complaint, denied.

70. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations of this paragraph of the Complaint, and therefore denies same. Denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS.

71. Admitted that DMI and IntegraLink attempted to pull data by unauthorized means from Reynolds's DMS for some period of time prior to 2015. Denied that DMI and IntegraLink ceased engaging in that activity as a result of a contractual agreement. As to the remaining allegations in this paragraph of the Complaint regarding CDK's ongoing data pulling activities, Reynolds lacks sufficient knowledge or information to form a belief about the truth of those allegations, and therefore denies same. Further denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS. In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and

Authenticom elected not to replead it. As to any remaining allegations of this paragraph of the Complaint, denied.

72. Denied in part. Admitted that the quoted statements appear in the cited press release from 2007 and that the National Auto Dealers Association ("NADA") and the American International Automobile Dealers Association ("AIADA") are two of the largest automobile dealer associations in the U.S. However, these quoted statements read in their entirety do not reflect the policies of these organizations today, more than a decade later. Reynolds further denies that Authenticom has fairly characterized the article, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

73. Denied in part. Admitted that certain individual dealers have stated that they believe they control who has access to their data, but denied that dealers are authorized to grant third parties access to Reynolds DMS platforms or that all dealers believe that third parties should have access to the DMS. As to the quotation from a Lexus dealership in California, Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations of this paragraph of the Complaint, and therefore denies same. As to any remaining allegations of this paragraph of the Complaint, denied.

74. Denied in part. Admitted that the quotes appear in the cited article. Denied that Authenticom has fairly characterized Chrysler's view in 2007, and denied that Chrysler's view in 2017 or 2018 remains the same. Further denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS. As to any remaining allegations of this paragraph of the Complaint, denied.

75. Denied in part. Admitted that the first quoted statement appears in a press release attributed to Open Secure Access, Inc. and that the remaining quoted statements purport to be from an Open Secure Access webpage from 2007 (but which is not available today). Reynolds denies that Open Secure Access's stated views are correct or appropriate. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations of this paragraph of the Complaint, and therefore denies same.

5. Participants in the Dealer Data Integration Market

76. Denied.

a. Authenticom

77. Denied in part. Upon information and belief, admitted that Authenticom was founded in 2002 by Steve Cottrell. Admitted that in October 2006, Authenticom claimed to serve more than 15,000 dealerships and nearly 500 vendor partners (but lack sufficient knowledge as to the truth of this). Admitted that Authenticom has accessed data stored on the Reynolds DMS platform using dealer login credentials in violation of dealer agreements with Reynolds, as well as federal law, state law, and the common law. Denied that there is any "industry standard" that could or does treat the usage of username-and-password access as appropriate. Admitted that Authenticom reported more than $18M in revenue during its fiscal year 2014. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations regarding Authenticom's actual revenue, customer, dealership, or employee numbers, and therefore denies same. As to all remaining allegations of this paragraph of the Complaint, denied.

78. Denied in part. Admitted that Authenticom operates a product called "DealerVault" that purports to manage the distribution and syndication of data to third party vendors. Denied that Authenticom has valid authorization to pull data directly from the Reynolds DMS or otherwise access the Reynolds DMS. Reynolds lacks knowledge or information sufficient

to form a belief about the truth of the remaining allegations of this paragraph of the Complaint, and therefore denies same.

79. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations of this paragraph of the Complaint, and therefore denies same.

80. Denied in part. Admitted that Authenticom's purported Terms and Conditions governing DealerVault (Pl. Ex. 28) state that "DealerVault shall only extract the Dealership Data that the Dealership permits DealerVault to extract," *id.* § 3.4, that "DealerVault may only disclose Dealership Data to third parties as authorized by Dealership or as required by law," and that "Dealership will retain all ownership of Dealership Data that Dealership submits to DealerVault …," *id.* § 5.3. However, denied that Authenticom complies with these provisions. Further denied that Authenticom extracts only that data that the dealer has specifically authorized Authenticom to pull. And denied that dealers can validly authorize Authenticom to pull data directly from the Reynolds DMS or otherwise access or utilize the Reynolds DMS. Authenticom specifically notes in its standard contract that it is not an agent. Reynolds lacks knowledge or information as to whether these terms are present in all Authenticom or DealerVault contracts. As to any remaining allegations of this paragraph of the Complaint, denied.

81. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations of this paragraph of the Complaint, and therefore denies same.

82. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations of this paragraph of the Complaint, and therefore denies same.

83. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations of this paragraph of the Complaint, and therefore denies same.

84. As to the first and last sentences of this paragraph of the Complaint, denied. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations of this paragraph of the Complaint, and therefore denies same.

85. Denied.

86. Admitted that the quotations were made by then-President Obama. Reynolds denies, however, that Authenticom has fairly characterized the article, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

87. Admitted that then-President Obama made the referenced speech on July 2, 2015; otherwise, denied. In addition, the core allegations in this Complaint (what the paragraph alleges "this lawsuit is about") regarding an alleged illegal market division agreement have been rejected by the Court and Authenticom has elected not to replead them.

b. CDK

88. Admitted that CDK owns DMI and IntegraLink and has a program called 3PA as part of its DMS; otherwise, denied.

i. Digital Motorworks and IntegraLink

89. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

90. Admitted that Mr. Distelhorst was formerly a Reynolds employee. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

91. Admitted that DMI and IntegraLink attempted to pull data from Reynolds's DMS by unauthorized means for some period of time prior to 2015. Denied that DMI and IntegraLink ceased engaging in that activity as a result of a contractual agreement. Reynolds otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in this

paragraph of the Complaint, and therefore denies same. In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and Authenticom elected not to replead it.

92. Denied. Reynolds has prohibited and sought to block unauthorized third-party access to its DMS for all of the relevant time period and before. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the other allegations in this paragraph of the Complaint concerning CDK, and therefore denies same. As to any remaining allegations of this paragraph of the Complaint, denied.

93. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

94. Denied. In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and Authenticom elected not to replead it.

95. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

ii. CDK Third Party Access Program

96. Admitted that CDK has a program known as 3PA. Reynolds otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

97. Denied that CDK and Reynolds entered into an illegal agreement. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

98. Denied that any changes CDK made to its 3PA program were at all related to the Data Exchange Agreement or any other agreement with Reynolds. Reynolds lacks knowledge or

information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

99. Admitted that CDK announced a "SecurityFirst" initiative on June 22, 2015. Reynolds otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

100. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

101. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

c. Reynolds Certified Interface Program

102. Admitted that Reynolds's RCI is a system of uniquely designed custom interfaces that form an integral part of the Reynolds DMS, through which third parties receive and send certain types of data to the DMS (though they do not have direct access to the DMS, by design). Admitted that Reynolds does not have an independent "data integration" business that pulls data from other DMS platforms and that Reynolds does not compete with DMI or IntegraLink. Denied that Mr. Brockman acquired Reynolds. Denied that Reynolds has ever allowed third parties to freely access its DMS. Admitted that CDK rigorously competes against Reynolds for DMS business, but Reynolds otherwise lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint as it relates to CDK, and therefore denies same. As to all remaining allegations of this paragraph of the Complaint, denied.

103. Denied.

104. Admitted that Reynolds's RCI pricing is not publicized and that it is determined based on the specific scope (and burdens) of each vendor's integration needs. Otherwise, denied.

105. Admitted that Reynolds has a tool called "Dynamic Reporting," which allows dealers to generate data reports. Denied that dealers must manually generate the reports—Dynamic Reporting allows dealers to schedule reports to run automatically up to four times a day. Denied to the extent that this paragraph implies that Dynamic Reporting is the only data exporting tool available to dealers in the Reynolds DMS. Admitted that Dynamic Reporting does not support "bi-directional feeds," but denied that it is purely a reporting tool—among other things, Dynamic Reporting allows a dealer to download the data to a PC in many different formats. Admitted that dealers must arrange a method to provide the generated reports to Authenticom, but denied that this process is too burdensome for dealers to use. As to all remaining allegations of this paragraph of the Complaint, denied.

d. The Remaining Data Integration Providers Have Been Driven from the Market by CDK and Reynolds

106. Denied that the "Dealer Data Integration Market" is a relevant and distinct economic market for any purpose in this case, and especially with regard to Reynolds's DMS. Admitted that there have been (and continue to be) a number of companies that have charged vendors and/or dealers to access various DMS platforms to pull and push data. As to all remaining allegations of this paragraph of the Complaint, denied.

107. Admitted that Reynolds sued SIS in 2012 for tortious interference and violation of the Computer Fraud and Abuse Act, among other things. As to all remaining allegations of this paragraph of the Complaint, denied.

108. Admitted on information and belief that SelectQu is owned by Dominion Enterprises, which also owns a number of applications and a competing DMS. Otherwise, denied.

109. Denied.

110. Denied.

C. The Single-Brand Aftermarkets for Dealer Data Integration Services

111. Denied.

112. Denied.

113. Denied.

114. Admitted that Reynolds's RCI contracts contain confidentiality provisions; otherwise, denied.

115. Denied.

116. Denied. In addition, Authenticom's core "market division" theory and exclusive dealing in dealer contracts theory described in this paragraph have been rejected by the Court and Authenticom elected not to replead them.

II. CDK and Reynolds Have Illegally Agreed To Eliminate Competition in the Dealer Data Integration Market and the Single-Brand Aftermarkets

A. The Facts of the Agreement Are Straightforward

117. To the extent this Paragraph purports to refer to Defendants' Data Exchange Agreement, admitted that this agreement was entered into in February 2015, but denied as to all characterizations of this agreement in this paragraph of the Complaint. As to all remaining allegations of this paragraph of the Complaint, denied.

118. Denied. In addition, Authenticom's core "market division" theory and exclusive dealing in dealer contracts theory described in this paragraph have been rejected by the Court and Authenticom elected not to replead them.

119. Denied. In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and Authenticom elected not to replead it.

120. Denied.

121. Denied.

B. The Purpose of the Agreement Is to Capture Monopoly Profits

122. Denied.

1. CDK and Reynolds Are Protecting Their DMS Duopoly

123. Denied.

124. Denied.

2. CDK and Reynolds Are Protecting Their Dealer Data Integration Monopolies

125. Denied.

126. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

127. Admitted that the quoted language appears in the cited hearsay publications. Reynolds denies, however, that Authenticom has fairly characterized the publications (or the facts), which speak for themselves. Reynolds denies all other allegations of this paragraph of the Complaint.

128. Denied.

129. Admitted that the quoted language appears in the cited publication, published in 2013. Reynolds denies, however, that Authenticom has fairly characterized the publication (or the facts), which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

130. Denied.

III. The Evidence of Defendants' Agreement to Eliminate Competition in the Dealer Data Integration Market and the Single-Brand Aftermarkets Is Overwhelming

131. Denied. In addition, Authenticom's core "market division" theory and exclusive dealing in dealer contracts theory described in this paragraph have been rejected by the Court and Authenticom elected not to replead them.

A. CDK and Reynolds Entered into a Per Se Illegal Written Agreement Dividing the Dealer Data Integration Market and Single-Brand Aftermarkets

132. To the extent this Paragraph purports to refer to Defendants' Data Exchange Agreement, admitted that this agreement was entered into in February 2015, but denied as to all characterizations of this agreement in this paragraph of the Complaint. As to all remaining allegations of this paragraph of the Complaint, denied.

133. Denied.

1. The Agreement Contains Specific Provisions Dividing the Dealer Data Integration Market

134. Denied. The statement quoted in the first sentence of this Paragraph does not appear in the Data Exchange Agreement at all. The statement quoted in the second sentence of this Paragraph is incomplete and therefore misleading. The Data Exchange Agreement's recitals state, among other things, that "CDK also provides DMI Third Party Clients with a data service that involves the polling of data from Reynolds DMS by CDK's IntegraLink and DMI affiliates (collectively 'DMI') for use by such automotive manufacturers or other third parties[.]" Nowhere in the Agreement does it state that CDK will stop providing these services. The Complaint is based upon an agreement that was never entered and Authenticom has refused to amend the Complaint in light of this and other core known misstatements in the Complaint despite access to millions of pages of documents (including the actual agreement), the Seventh Circuit's rejection of its theory of injunctive relief, and the partial dismissal of some of its claims (including its core market division theory). In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and Authenticom elected not to replead it or any of its other claims to correct its material misstatements.

135. Denied in part. The Data Exchange Agreement does not contain the quoted language in the last sentence of this Paragraph, or any provision to that effect. Authenticom has

refused to replead to correct its misstatements. However, the Data Exchange Agreement defines a "Wind Down Period" (subject to extension by agreement of the parties) during which Reynolds agreed to, on an interim basis, "protect and facilitate current Reynolds DMS access by CDK and DMI Third Party Clients and CDK Applications," and to "not take any measures to block or otherwise disrupt DMI's normal Reynolds DMS access during such Wind Down Period" subject to certain conditions. In addition, CDK's ability to access the Reynolds's DMS during the specified wind-down period was subject to the various restrictions, protections, and requirements set forth in the Agreement. All of those interim measures, along with the Wind Down Period, have now terminated. As to all remaining allegations of this paragraph of the Complaint, denied.

2. The Agreement Required Coordination in Transitioning Vendor Clients from CDK to Reynolds

136. Denied in part. During the Wind Down Period, CDK agreed "to reasonably cooperate with Reynolds's efforts, if any, to have Third Party Clients execute agreements to become part of the Reynolds RCI Program[.]" The second quoted statement does not appear in the Data Exchange Agreement. The meaning of the Agreement speaks for itself. As to all remaining allegations of this paragraph of the Complaint, denied.

137. Denied.

138. Denied in part. Upon entering into the Data Exchange Agreement, CDK agreed to provide Reynolds with a list of the dealer login credentials that it planned to use during the Wind Down Period and certain information about its vendor clients. CDK was not required as to provide the stipulated vendor information to Reynolds, but the information was a requirement for Reynolds's ability to provide an interim solution for such connections. Reynolds otherwise denies the remaining allegations in this paragraph of the Complaint.

3. CDK and Reynolds Implemented the Agreement

139. Denied in part. Upon information and belief, CDK stopped attempting to access Reynolds's DMS because it is illegal, because it is immoral, and because CDK lacks the technical ability to do so—not because of any agreement.

140. Denied that "[c]onsistent with their agreement, CDK and Reynolds coordinated the transition of vendors from CDK to Reynolds." Upon information and belief, CDK sent a letter to its vendor clients on or about March 2, 2015. That letter speaks for itself. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

141. Upon information and belief, admitted that CDK sent a letter including the quoted language on or about April 2, 2015. Reynolds denies, however, that Authenticom has fairly characterized the letter, which speaks for itself. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

142. Upon information and belief, admitted that CDK sent a letter including the quoted language. Reynolds denies, however, that Authenticom has fairly characterized the letter, which speaks for itself. Denied that the letter gave a deadline by when the vendors needed to enroll in the RCI program. As to all remaining allegations of this paragraph of the Complaint, denied.

143. Upon information and belief, admitted that CDK sent a letter including the quoted language. Reynolds denies, however, that Authenticom has fairly characterized the letter, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

144. Upon information and belief, admitted that the referenced CDK letter contains the quoted language, taken out of context. Reynolds denies, however, that Authenticom has fairly characterized the letter, which speaks for itself. Admitted that Reynolds created an interim

solution, subject to strict requirements and controls, for eligible vendors to receive data through DMI until a more stable and secure RCI interface could be built; denied that doing so in any way undermines the substantial security and stability benefits that RCI generally provides to Reynolds's DMS. Reynolds denies all other allegations of this paragraph of the Complaint.

145. Upon information and belief, admitted that the referenced CDK letter contains the quoted language, taken out of context. Reynolds denies, however, that Authenticom has fairly characterized the letter, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

146. Denied in part. Admitted that Reynolds sent letters to certain vendors with whom it was negotiating, but denied that CDK played any role in that negotiation process. As to all remaining allegations of this paragraph of the Complaint, denied.

147. Denied.

148. Denied. In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and Authenticom elected not to replead it.

B. CDK and Reynolds Require Dealers and Vendors to Enter into Exclusive Dealing Arrangements That Are Patently Anticompetitive

149. Denied as to Reynolds. As to CDK, Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, Authenticom's core "market division" theory and exclusive dealing in dealer contracts theory described in this paragraph have been rejected by the Court and Authenticom elected not to replead them.

1. Defendants' DMS Contracts with Dealers Grant Defendants an Exclusive Right to Access the Dealers' Data

a. The Dealer Exclusive Dealing Terms

150. Denied as to Reynolds. Dealers are not authorized to provide third parties with access to the DMS, but they can provide their data to third parties in any other way, including with the assistance of multiple reporting tools within the DMS. As to CDK, Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

151. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. However, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

152. Reynolds admits that the quoted language in this paragraph of the Complaint appears in the referenced documents, subject to the clarification that the right to access, copy, or use the dealer's Business Data is "in the course of providing certain agreed upon DMS-related services for the dealership." Reynolds denies, however, that Authenticom has accurately characterized the referenced documents, which speak for themselves. Reynolds further admits that the provisions described in this paragraph of the Complaint typically last as long as the Reynolds DMS contract, but denies that the length of those contracts is typically five to seven years. Rather, the length of those contracts is an entirely negotiable term of the licensing agreement and can be less than 5 years. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

b. CDK and Reynolds Vigorously Enforce the Dealer Exclusive Dealing Provisions

153. Reynolds admits that it enforces the terms of its DMS contracts. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

154. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

155. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. However, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

156. Reynolds admits that it informed Authenticom in an April 6, 2015 letter that Reynolds had become aware of specific evidence of tortious interference of its contracts by Authenticom (along with other legal violations), and that such letter included the quoted language. Reynolds further admits that it sued SIS in 2012 for its illegal tortious interference and violation of the Computer Fraud and Abuse Act, among other things, as a result of SIS's attempts to access the Reynolds DMS without proper authorization. Reynolds also admits that its security protocols

disable unauthorized automated access to the Reynolds DMS. Reynolds otherwise denies all other allegations of this paragraph of the Complaint. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

2. Defendants' Contracts with Vendors Grant Defendants an Exclusive Right to Provide Data to Vendors

157. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

158. Denied as to Reynolds. Reynolds's RCI agreements do not contain "exclusive dealing provisions" and do not prohibit vendors from receiving data in other authorized ways, including through dealers' use of, for example, the Reynolds-provided Dynamic Reporting functions. Reynolds's RCI agreements also place no restrictions on how vendors send or receive data from other DMS platforms, including CDK's. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

a. The Vendor Exclusive Dealing Terms

159. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

160. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

161. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

162. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

163. Reynolds admits that the quoted language in this paragraph of the Complaint appears in the referenced document. Reynolds denies, however, that Authenticom has accurately characterized the referenced document, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

164. Reynolds admits that the quoted language in this paragraph of the Complaint appears in the referenced document. Reynolds denies, however, that Authenticom has accurately characterized the referenced document, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

165. Reynolds admits that it receives appropriate audit rights under the RCI contract for legitimate business purposes, including related to data privacy and security. Reynolds denies, however, that Authenticom has accurately characterized the referenced document, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

b. Defendants' Vendor Contracts Contain Price Secrecy Provisions That Prohibit Vendors from Informing Dealers About the Data Fees

166. Reynolds admits that the price (and other) terms of the RCI contract are confidential, pursuant to the terms of the contract. Reynolds denies, however, that Authenticom has accurately characterized the referenced document, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

167. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

168. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

169. Admitted that the contracts contain confidentiality provisions. Reynolds lacks knowledge or information sufficient to form a belief about whether this is "similar[]" to the CDK contract, and therefore denies same.

170. Denied.

c. CDK and Reynolds Vigorously Enforce the Vendor Exclusive Dealing and Price Secrecy Provisions

171. Reynolds admits that it enforces its contractual rights vis-a-vis vendors as appropriate and negotiates resolutions and/or invokes its dispute resolution rights under the relevant contracts. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

172. Reynolds admits that in August 2016, Reynolds sent a vendor a letter containing the quoted language. Reynolds denies, however, that Authenticom has accurately characterized the referenced document, which speaks for itself, or the context in which the letter was sent. Reynolds denies all other allegations of this paragraph of the Complaint.

173. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

174. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

3. The Dealer and Vendor Exclusive Dealing and Price Secrecy Provisions Are Anticompetitive

175. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

176. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

177. Reynolds admits that the standard Reynolds RCI contract recites a duration of three years with automatic renewals for one-year terms. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

C. Defendants Are Engaged in a Coordinated Campaign to Block Authenticom's Access to Dealer Data and Thereby Destroy Its Business

178. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

1. Defendants Have Admitted That They Have Agreed to Restrict Access and Block Authenticom

179. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

180. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. However, with respect to the allegation regarding exclusive dealing, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

181. Denied as to Reynolds. On information and belief, admitted that some other DMS providers allow Authenticom to access their respective DMS platforms in various ways, but denied that those DMS providers doing so recognizes or creates a right for Authenticom to access Reynolds's proprietary DMS without Reynolds's authorization. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

2. Defendants' Employees Are Working In Concert to Coordinate the Blocking of Authenticom

182. Denied.

183. Reynolds admits that Steve French previously worked for Reynolds as a data collections manager until 1998, when he joined IntegraLink. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

3. Defendants Tried to Coerce Authenticom to Exit the Dealer Data Integration Market

184. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

185. Reynolds admits that it informed Authenticom in an April 6, 2015 letter that Reynolds had become aware of specific evidence of tortious interference of its contracts by Authenticom (and other illegal acts); that Authenticom's response contained the quoted language; and that (as instructed by Mr. Cottrell) on May 7, 2015, Reynolds's lawyer sent a proposed agreement to settle disputed claims to Mr. Cottrell's lawyer with a cc to Mr. Cottrell (as requested by Mr. Cottrell). Reynolds denies, however, that Authenticom has accurately characterized the referenced documents, which speak for themselves. Reynolds otherwise denies all other allegations of this paragraph of the Complaint as they relate to Reynolds.

186. Reynolds admits that Authenticom ultimately did not sign any settlement agreement. Reynolds denies all other allegations of this paragraph of the Complaint.

4. Defendants Are Blocking Authenticom's Ability to Provide Dealer Data Integration Services

187. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

a. CDK and Reynolds Have Disabled Authenticom's Usernames En Masse

188. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

189. Reynolds admits that it has undertaken efforts to enforce its longstanding policies and contracts prohibiting unauthorized third-party DMS access; that Reynolds disabled Authenticom's usernames in 2009, when it introduced "challenge questions" and "captcha" (where

the user has to enter random blurred text) to prevent unauthorized and automated access to Reynolds's DMS; that in June 2013, Reynolds's security protocols disabled Authenticom's, CDK's, and other integrators' login credentials; and that Reynolds's security protocols disabled a substantial number of suspicious user IDs during the summer of 2013. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

b. Dealers Have Protested to CDK and Reynolds and Demanded That They Stop Blocking Authenticom

190. Reynolds admits that certain dealers sometimes complain about third-party access policies. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

191. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. Further denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS.

192. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. Further denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS.

193. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. Further denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS.

194. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. Further denied to the extent that this paragraph implies that dealers own all categories of data processed by the DMS. Denied to the extent this paragraph implies that dealers may control access to a proprietary DMS. Also denied that dealers lack the ability to choose a DMS provider that allows them to use Authenticom's data polling services.

c. Dealers Have Set Up New Usernames for Authenticom, but Those Have Been Quickly Blocked by CDK and Reynolds Too

195. Reynolds admits on information and belief that when it disabled usernames and passwords wrongfully used by Authenticom, Authenticom responded by developing new ways to circumvent Reynolds's security protocols and by encouraging dealers to issue new usernames and passwords to Authenticom (or provide administrator-level passwords to Authenticom so that it could re-enable passwords or create new ones) in direct violation of dealer agreements. Reynolds further admits that it employs security protocols that endeavor to identify and block all unauthorized and automated login attempts to the DMS. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

196. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

197. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

d. CDK and Reynolds Have Refused To Give Credence to the Dealers' Objections

198. Admitted that Reynolds enforces the terms of its DMS contracts; otherwise, denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

199. Reynolds admits that it employs security protocols that endeavor to identify and block unauthorized and automated login attempts to the DMS. Reynolds otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

e. CDK and Reynolds Are Proactively Contacting Dealers Served by Authenticom to Pressure Them to Have Their Vendors Switch to the RCI and 3PA Programs

200. Reynolds admits that it has discussed the benefits of RCI integration with its dealership customers (and the industry generally) throughout the history of its security and technology enhancements. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

201. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

202. Reynolds admits that it sent a communication containing the quoted language, with the correction that "impacted by this" should read "impacted by this change" and that the quote lacks context. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

f. CDK and Reynolds Have Spread False Information About Authenticom's Security as Part of Their Marketing Push

203. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

204. Admitted that allowing third parties automated access to the DMS creates risks to the DMS and to dealers; otherwise denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

205. Admitted that Authenticom has pulled data for Reynolds-owned applications in certain scenarios but no longer does so; otherwise denied.

206. Reynolds admits that AVRS, Inc. ("AVRS") is a subsidiary of Computerized Vehicle Registration ("CVR") which, in turn, is a joint venture between CDK and Reynolds, that provides electronic vehicle and titling services ("EVR") in California and that AVRS was using Authenticom for certain services at the time of CVR's acquisition of AVRS in 2015. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

207. Reynolds admits that it previously used Authenticom to pull data from other DMS providers' systems, so long as those DMS providers (and associated dealers) had authorized Authenticom to do so. Reynolds denies all other allegations of this paragraph of the Complaint.

g. Authenticom Is Losing Its Customers – and Therefore Its Business – Because of Defendants' Actions

208. Denied.

209. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

210. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

IV. Defendants' Actions Have Harmed Competition

211. Denied.

A. Defendants' Anticompetitive Conduct Has Resulted in Massive Price Increases in the Dealer Data Integration Market

212. Denied.

213. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

1. CDK and Reynolds Have Imposed Massive Price Increases As Compared to What Authenticom Charged

214. Reynolds admits that certain "data integrators," as Authenticom defines that term (which Reynolds denies), charge vendors per dealership rooftop. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

215. Reynolds denies that its prices for once-daily batch data are "far higher" than Authenticom's prices. Reynolds admits that real-time or more comprehensive RCI interfaces are typically higher in price, but denies that such services are comparable to Authenticom's unauthorized, bootleg screen-scraping. Reynolds further denies that any vendor was "forced" to join the RCI program. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

216. Reynolds denies that it charges vendors enormous upfront fees to initiate services; Reynolds charges vendors reasonable fees for certification and installation services. Reynolds further denies that it typically charges at least $30,000 to join the RCI program. Reynolds admits that it charges approximately $300 set-up fees, depending on the volume of work anticipated to build the custom interface(s). Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

2. CDK and Reynolds Have Dramatically Increased the Prices for Their Own Data Integration Services

217. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, Authenticom's core "market division" theory described in this paragraph has been rejected by the Court and Authenticom elected not to replead it.

218. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

219. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

220. Reynolds admits that it charges a small per-transaction fee for write-back transmissions only, in a (largely successful) effort to incentivize vendors to ease the operational load on the DMS system from inefficient data pushes and recover significant costs of monitoring real-time data pushes. Reynolds further admits that it generally raised RCI prices in 2013 for certain categories of applications, but did so to reflect the program's costs, benefits, and system burdens. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

3. The Evidence of CDK's and Reynolds' Price Increases Is Overwhelming

221. Reynolds admits that the industry press has reported on pricing under CDK's and Reynolds's respective programs, but notes that its reporting has been inaccurate and largely taken out of context. Reynolds denies all other allegations of this paragraph of the Complaint.

222. The hearsay articles speak for themselves. Denied as to the truth of the allegations in this paragraph of the Complaint regarding Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint regarding CDK, and therefore denies same.

223. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same.

4. CDK and Reynolds Continue to Charge Dealers Escalating Fees for DMS Services

224. Reynolds admits, on information and belief, that some vendors pass through some, all, or none of their integration fees. Other vendors mark up the fees. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks

knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

225. Reynolds admits that it has fee escalation clauses in its DMS contracts with dealers, with the clarification that Reynolds's DMS fees are whatever Reynolds and its customers contractually negotiate. Reynolds admits that the standard Reynolds contract provides that DMS fees go up every year on March 1, measured by the Customer Price Index plus 2%. Reynolds denies, however, that Authenticom has fairly characterized Reynolds's contract, which speaks for itself. Reynolds further denies that it imposes "rapidly escalating data integration fees" and "price hikes." Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. As to any remaining allegations of this paragraph of the Complaint, denied.

B. Defendants' Anticompetitive Conduct Has Harmed Competition in Many Other Ways

226. Denied.

227. Denied as to Reynolds. The Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

228. Reynolds admits that it has a per-transaction fee pertaining to data write-backs and that vendors are economizing their write-backs accordingly, but Reynolds denies that this per-transaction fee applies to data being sent to vendors. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

229. Denied.

230. Denied.

231. Denied.

V. Authenticom Has Suffered Antitrust Injury

232. Denied. In addition, the Court has previously rejected the dealer contract exclusive dealing theory and Authenticom has elected not to replead it.

233. Denied as to Reynolds. Upon information and belief, Reynolds denies that Authenticom is "cash flow insolvent" or otherwise on the brink of demise. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

VI. Defendants' Anticompetitive Conduct Has No Pro-Competitive Justification

234. Denied.

235. Reynolds admits that data security concerns are an important reason, among several others including system stability, data integrity, and intellectual property, why Reynolds does not permit unauthorized third-party access to its DMS platform. Further admitted that Authenticom's role as a system access "intermediary" creates unnecessary security risks, along with other risks, costs, and unjust enrichment to Authenticom. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same. In addition, Authenticom's core "market division" theory and exclusive dealing in dealer contracts theory described in this paragraph have been rejected by the Court and Authenticom elected not to replead them.

236. Denied.

237. Denied as to Reynolds. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in this paragraph of the Complaint, and therefore denies same.

238. Admitted that the quoted statements appear in the referenced documents. Reynolds denies, however, that Authenticom has properly characterized those documents, and all other allegations in this paragraph are denied.

239. Reynolds admits that the quoted language appears in the referenced article. Reynolds denies, however, that Authenticom has fairly characterized the article, which speaks for itself. Reynolds denies all other allegations of this paragraph of the Complaint.

240. Admitted that Authenticom purports to have (or had) a $20 million cyber liability insurance policy; denied that Authenticom has properly characterized the scope and coverage of those policies, which speak for themselves. Otherwise, denied.

241. Reynolds admits that it has used Authenticom to pull data for Reynolds-owned applications in certain limited situations; denied that doing so implied that Reynolds in any way believed Authenticom's efforts to access Reynolds's DMS without Reynolds's authorization were secure or appropriate. Reynolds denies all other allegations of this paragraph of the Complaint as they relate to Reynolds.

FIRST CAUSE OF ACTION:
HORIZONTAL CONSPIRACY IN VIOLATION OF
SECTION 1 OF THE SHERMAN ACT

242. Paragraph 242 incorporates by reference the preceding allegations of the Complaint; Reynolds likewise restates and incorporates by reference its responses above to those paragraphs. This cause of action, to the extent that it is based on a market allocation theory, has been dismissed and has not been repleaded by Authenticom.

243. Denied.

244. Admitted that Reynolds and CDK are horizontal competitors in the DMS market; otherwise, denied.

245. Denied.

246. Denied.

247. Denied.

248. Denied.

249. Denied.

250. Denied.

251. Denied.

252. Denied.

SECOND CAUSE OF ACTION:
EXCLUSIVE DEALING PROVISIONS IN VIOLATION OF SECTION 1 OF THE SHERMAN ACT

253. Paragraph 253 incorporates by reference the preceding allegations of the Complaint; Reynolds likewise restates and incorporates by reference its responses above to those paragraphs. This claim, to the extent based upon dealer contracts, has been dismissed and has not been repleaded by Authenticom.

254. Denied.

255. Denied.

256. Denied.

257. Denied.

258. Denied.

259. Denied.

260. Denied.

261. Denied.

THIRD CAUSE OF ACTION:
ILLEGAL TYING IN VIOLATION OF SECTION 1 OF THE SHERMAN ACT

262. Paragraph 262 incorporates by reference the preceding allegations of the Complaint; Reynolds likewise restates and incorporates by reference its responses above to those paragraphs. This claim has been dismissed in its entirety and has not been repleaded by Authenticom.

263. Denied.

264. Denied.

265. Denied.

266. Denied.

267. Denied.

268. Denied.

269. Denied.

FOURTH CAUSE OF ACTION:
MONOPOLIZATION OF THE DEALER DATA INTEGRATION AFTERMARKETS IN VIOLATION OF SECTION 2 OF THE SHERMAN ACT

270. Paragraph 270 incorporates by reference the preceding allegations of the Complaint; Reynolds likewise restates and incorporates by reference its responses above to those paragraphs.

271. Denied.

272. Denied.

273. Denied.

274. Denied.

275. Denied.

276. Denied.

FIFTH CAUSE OF ACTION:
TORTIOUS INTERFERENCE

277. Paragraph 277 incorporates by reference the preceding allegations of the Complaint; Reynolds likewise restates and incorporates by reference its responses above to those paragraphs.

278. Denied.

279. Reynolds lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph of the Complaint, and therefore denies same. Further denied that dealers that licensed Reynolds's DMS can validly authorize Authenticom to access or use Reynolds's DMS.

280. Denied.

281. Denied.

282. Denied.

283. Denied.

284. Denied.

285. Denied.

286. Denied.

RESPONSE TO PRAYER FOR RELIEF

Authenticom is not entitled to any of the requests included in its Prayer for Relief.

AFFIRMATIVE DEFENSES

Reynolds pleads the following affirmative defenses to the allegations in the Complaint:

FIRST AFFIRMATIVE DEFENSE

(Failure to State a Claim)

1. Authenticom has failed to state ultimate facts sufficient to constitute a claim for relief. Facts in support of this affirmative defense are set forth in Defendant The Reynolds and Reynolds Company's Memorandum in Support of Its Motion to Dismiss Plaintiff Authenticom, Inc.'s Original Complaint. *See generally* Case No. 18-cv-868, ECF No. 176; Order, Case No. 18-cv-864, ECF No. 176.

SECOND AFFIRMATIVE DEFENSE
(Lack of Plausibility)

2. Authenticom's claims are not plausible under *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007) and its progeny. Facts in support of this affirmative defense are set forth in Defendant The Reynolds and Reynolds Company's Memorandum in Support of Its Motion to Dismiss Plaintiff Authenticom, Inc.'s Original Complaint. *See generally* Case No. 18−cv−868, ECF No. 176.

THIRD AFFIRMATIVE DEFENSE
(Illegality and Lack of Antitrust Injury)

3. Because Authenticom's actions are illegal independent of any Reynolds activity challenged by Authenticom, all of Authenticom's claims are barred as a matter of law. Authenticom has engaged in illegal and unethical activity and has acted and is acting in bad faith with respect to the subject of this dispute. Authenticom's relentless, ongoing, unauthorized attempts to hack into Reynolds's DMS, utilize its copyrighted software, and "scrape" data for sale to third-party vendors is illegal under federal and state law. Authenticom's actions are illegal as set forth more fully in the Counterclaims below. Restraint of illegal trade is not an antitrust violation, and because Authenticom's claims against Reynolds are based on Authenticom's illegal business, Authenticom lacks any valid antitrust injury. Further, Authenticom has brazenly ignored

Reynolds's repeated objections and continued with its technological gamesmanship to circumvent Reynolds's security protocols, resulting in increased expenses and DMS problems for Reynolds; it has knowingly and intentionally induced Reynolds's dealer customers into breaching their DMS license agreements to facilitate Authenticom's unauthorized access into the DMS; and it has enjoyed many of the benefits of the DMS without paying anything for access into it. *See generally* Counterclaims, *infra*.

FOURTH AFFIRMATIVE DEFENSE
(Laches)

4. Authenticom's claims are barred by the doctrine of laches. Authenticom's complaint alleges claims against Reynolds that are based on actions and events dating back to 2007. The doctrine of laches bars Authenticom's claims given its unreasonable delay in bringing its claims.

FIFTH AFFIRMATIVE DEFENSE
(Waiver and/or Equitable Estoppel)

5. Authenticom's claims are barred by the doctrines of waiver and/or equitable estoppel. Authenticom's complaint alleges claims against Reynolds that are based on actions and events dating back to 2007. Authenticom's failure to raise these claims earlier constitutes waiver. In addition, Authenticom is equitably estopped from raising these claims.

SIXTH AFFIRMATIVE DEFENSE
(Statute of Limitations)

6. Authenticom's claims are barred by the applicable statutes of limitations. Authenticom's complaint alleges claims against Reynolds that are based on actions and events dating back to 2007. The statutory time applicable to each of Authenticom's claims has passed and its claims are time-barred.

SEVENTH AFFIRMATIVE DEFENSE
(Failure of Causation)

7. Authenticom's claims fail due to a lack of causation. Among other things, such failures include the following:

8. Authenticom's alleged financial distress is principally caused by Authenticom's own decision to take out an aggressively large loan in 2014, the proceeds of which Authenticom used to buy out several dissenting investors, thereby increasing Mr. Cottrell's ownership stake in the company. Reynolds bears no responsibility for Authenticom's poor financial decisions—especially given that Authenticom was fully aware of Reynolds's prohibition on third-party access to the Reynolds DMS prior to the decision to take out that loan.

9. Authenticom's claimed damages with respect to Reynolds are also barred by the plain terms of Reynolds's DMS license agreements with its dealers. As Authenticom admits, Reynolds's DMS licenses are limited to dealership employee end users alone, and the licenses prohibit granting any other persons or parties access to Reynolds's proprietary DMS software and systems. The Court dismissed Authenticom's claims with regard to Reynolds's DMS license agreements, and Authenticom elected not to replead, thereby conceding that such agreements are legal and enforceable. *See* Order, Case No. 18-cv-864, ECF No. 176. Thus, regardless of any claimed wrongdoing by Reynolds, Authenticom would have been (and continues to be) barred from accessing any Reynolds DMS by the terms of the Reynolds license agreements.

EIGHTH AFFIRMATIVE DEFENSE
(Failure to Mitigate Damages)

10. Authenticom bases its asserted antitrust violations against Reynolds on alleged business practices and contract terms that it says have been evident from publicly available information throughout the alleged relevant period. Assuming arguendo the truth of these allegations, Authenticom failed to mitigate its alleged damages by promptly filing suit, or by any other means. Therefore, Authenticom's claims should be dismissed, in whole or in part, and/or its

alleged damages reduced, because Authenticom failed to take all necessary, reasonable, and appropriate actions to mitigate its alleged damages.

NINTH AFFIRMATIVE DEFENSE
(Damages Are Too Speculative)

11. Authenticom has not suffered any legally cognizable injury and has not suffered an injury-in-fact. If and to the extent Authenticom has been damaged (which Reynolds denies), the amount of damages that Authenticom alleges to have suffered is too remote, speculative, and indirect from the alleged conduct to allow recovery, and it is impossible to ascertain, apportion, and allocate such damages with reasonable certainty.

TENTH AFFIRMATIVE DEFENSE
(Unavailability of Injunctive Relief)

12. Authenticom's claims for equitable relief are barred for the reasons set forth in the Seventh Circuit's opinion in this matter (*Authenticom, Inc. v. CDK Glob.*, LLC, 874 F.3d 1019 (7th Cir. 2017)), including *Verizon Communications Inc. v. Law Offices of Curtis v. Trinko*, 540 U.S. 398 (2004), and *Pacific Bell Telephone Co. v. Linkline Communications, Inc.*, 555 U.S. 438, (2009). In addition, Authenticom has suffered no irreparable harm and otherwise fails to satisfy the criteria necessary for injunctive relief.

ELEVENTH AFFIRMATIVE DEFENSE
(Unjust Enrichment)

13. Authenticom's claims are barred, in whole or in part, because any recovery would result in unjust enrichment to Authenticom, as detailed in Reynolds's counterclaims below.

TWELFTH AFFIRMATIVE DEFENSE
(Failure to Allege Market)

14. Authenticom's claims are barred, in whole or in part, because the Complaint has insufficiently alleged a relevant product market and geographic market and is so vague and ambiguous as to deny Reynolds notice of the markets alleged by Authenticom.

THIRTEENTH AFFIRMATIVE DEFENSE
(Reynolds's Actions Were Procompetitive)

15. Authenticom's claims are barred, in whole or in part, because Reynolds's conduct was pro-competitive, reasonable, and permissible. Reynolds's conduct was further based on independent, legitimate, and self-interested business and economic justifications.

FOURTEENTH AFFIRMATIVE DEFENSE
(Reynolds's Actions Did Not Lessen Competition)

16. Authenticom's claims are barred, in whole or in part, because none of Reynolds's alleged actions or omissions substantially lessened competition within any properly defined market.

FIFTEENTH AFFIRMATIVE DEFENSE
(Reynolds Did Not Cause Injury)

17. Authenticom's claims are barred, in whole or in part, because to the extent Authenticom suffered any injury or incurred any damages as alleged in the Complaint, which Reynolds denies, any such injury or damage was caused and brought about by the acts, conduct or omissions of individuals or entities other than Reynolds and, as such, any recovery herein should be precluded or diminished in proportion to the amount of fault attributable to such other individuals or entities.

SIXTEENTH AFFIRMATIVE DEFENSE
(Intervening Cause)

18. Authenticom's claims are barred, in whole or in part, because to the extent Authenticom suffered any injury or incurred any damages as alleged in the Complaint, which Reynolds denies, any such injury or damage was caused and brought about by intervening or superseding events, factors, occurrences, conditions or acts of others, including forces in the marketplace, and not by the alleged wrongful conduct on the part of Reynolds.

SEVENTEENTH AFFIRMATIVE DEFENSE
(Incorporation and Reservation of Defenses)

19. Reynolds incorporates by reference all affirmative defenses raised in all prior pleadings and filings, including but not limited to its Motion to Dismiss (Case No. 18−cv−868, Dkt. No. 176) and those raised by other parties and defendants. Reynolds further reserves the right to amend or supplement its affirmative defenses as discovery or further investigation may justify.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Reynolds hereby demands trial by jury on all issues so triable.

COUNTERPLAINTIFF THE REYNOLDS AND REYNOLDS COMPANY'S COUNTERCLAIMS

Reynolds, for its counterclaims against Authenticom, Inc. ("Authenticom"), states as follows:

1. The Reynolds and Reynolds Company expended enormous resources building and maintaining a high-end, highly-integrated, closely-controlled enterprise software and computing platform for automotive dealerships and dealership groups. In the industry, enterprise platforms for automotive dealerships are known as Dealer Management Systems or, more commonly, DMSs. The Reynolds DMS is a bespoke product and comprises more than 20 million lines of programming code. Today, the Reynolds DMS is distributed across more than 5,000 automobile dealers in North America, requiring constant maintenance, control, and monitoring of a complex, distributed computing network that Reynolds created, built, refined, improved and scaled over decades to achieve maximum performance, speed, stability and security.

2. For these reasons, among others, the Reynolds DMS is a premium product that commands a premium price. Reynolds licenses its DMS to its dealership customers under a strict set of terms and conditions designed to protect its system's functional integrity and security, protect Reynolds's valuable intellectual property rights, and meet Reynolds's contractual obligations to third parties. As a condition of this license, each Reynolds dealer agrees that the only persons allowed to access and use the DMS shall be dealership employees who use the DMS on a day-to-day basis to carry out their job functions. Dealers know and agree to this restriction (and others) when they choose to license a Reynolds DMS, and both Reynolds and the dealers negotiate the resulting licensing fees based on the expectation that the license's scope extends to dealership employees alone.

3. Reynolds's DMS is a premium product because it is significantly more stable, secure, and effective than similar products provided by its competitors. Though there are tens of thousands of new and used car dealerships in the United States, Reynolds sells its proprietary DMS primarily to larger car dealership groups that require a sophisticated, stable, and secure platform to manage the complex network of transactions (and vast cashflows) that move through their businesses. Reynolds's DMS gives these dealers numerous tools and functionalities that allow them to improve the profitability and efficiency of their operations.

4. Dealership operations, particularly those of Reynolds's target customers, generate and depend upon a swathe of critically sensitive private data, including consumer financial information far more detailed and voluminous than ordinary consumer transactions. By way of example, that information frequently includes credit scores, driver's license numbers, and Social Security Numbers. Protecting the integrity and security of the Reynolds platform, and the sensitive consumer financial data it contains, is a paramount concern for both Reynolds and its customers. Consistent with this concern, Reynolds's system includes multiple protections designed to exclude hackers, to prevent automated scripts from encumbering system resources, and to ensure that only properly licensed dealership employees can access and use the system.

5. While the Reynolds DMS has a great deal of native functionality for core dealership functions like vehicle sales, financing and insurance, and inventory management, dealers can choose to use certain third-party software applications that supplement or replace the DMS's native functionalities. Just as some smartphone users prefer to install Google Chrome on their iPhones instead of using the native Safari browser, some dealers might prefer a third party's contact management application to the Reynolds DMS's native program. Dealers regularly assess the availability and compatibility of their preferred third-party applications when choosing a DMS

platform. Accordingly, beginning in the early 2000s, Reynolds built a specialized functionality—today known as the Reynolds Certified Interface, or RCI, program—that enables third-party applications to function seamlessly with the Reynolds DMS. When an application vendor is approved to join the RCI program, Reynolds builds them customized software interfaces that allow the DMS and the application to communicate and exchange data in a secure and efficient manner. Dealers choosing a Reynolds DMS can easily determine if a particular third-party vendor is an available Reynolds RCI partner before making their DMS choice.

6. Each RCI interface package for each Reynolds RCI partner is precisely tailored to the corresponding application's needs, including the communication protocols, business rules, data elements, and the regularity of updates (such as integrated real-time and bi-directional capabilities, where necessary). Some application vendors purchase packages of ten or more interfaces, with each interface providing different functionalities and configured sets of data elements. The interfaces also run through a centralized hub, known as the Reynolds Integration Hub (RIH), which allows each data feed to be monitored, recorded, and supported with the requisite computing resources. Each certified vendor also signs a contract, known as a Reynolds Interface Agreement (RIA) that, among other things, contains a robust set of security requirements.

7. Reynolds charges (and has a right to charge) application vendors premium prices for its RCI interfaces. These prices recognize the tremendous value of the RCI interfaces—and packages of interfaces—as well as Reynolds's huge investments in building and maintaining those interfaces (as well as the rest of the Reynolds DMS). In this sense, Reynolds is no different from other computer system developers and operators that have spent years and millions of dollars to build secure access points and who, as a result of their investments in intellectual property, are free

both to charge for their systems and to refuse access to those who decline to pay for the license to use the system or who threaten its integrity and security.

8. Counterdefendant Authenticom, Inc. is aware of the contractual and license restrictions on access to the Reynolds DMS. Nonetheless, Authenticom's business model for Reynolds DMS customers is based on stolen access to the Reynolds system. On a daily basis, Authenticom tortiously interferes with Reynolds's contracts by inducing dealers to hand secure logins to Reynolds's system over to Authenticom, in what Authenticom knows is a breach of the dealers' license agreements with Reynolds. As explained herein, Authenticom then uses these misappropriated user IDs and passwords to run, log into, and use the Reynolds DMS, thereby fraudulently misrepresenting that it is an authorized dealership employee, bypassing critical access controls, and infringing Reynolds's copyrights. Authenticom next evades Reynolds's CAPTCHA and other access controls by, among other things, running a series of deceptive automated scripts that trick the system into believing that Authenticom is a bona fide—human—employee user in order to operate the DMS program and evade Reynolds's security measures. Authenticom then uses its automated software programs to activate the Reynolds system's robust reporting tools and other functionalities to hoover up information through screen-scraping and high-volume automated downloads of data.

9. Its electronic burglary having been accomplished, Authenticom then absconds with that information (much of it critically sensitive, none of it belonging to Authenticom) by exporting it to itself. With no evident sense of irony, Authenticom then sells the data and information it has obtained to third-party application vendors, who must agree to Authenticom's own licensing requirements but who—like Authenticom itself—have no license or right to use Reynolds's system in this manner.

10. Authenticom's business model for Reynolds's systems rests on an ongoing, intentional, and staggering level of computer fraud and theft from Reynolds. Authenticom's thievery is calculated and intentional: it admits in its pleadings that it has worked with Reynolds's licensed dealers to develop "workaround solutions that circumvented Reynolds's efforts to block access to the Reynolds system." Reynolds put Authenticom on notice that its actions were illegal and unauthorized and demanded that it cease and desist, but to no avail. Authenticom has now repackaged itself as the victim of anticompetitive restrictions, bringing a suit the premise of which is that Authenticom has been deprived of the ability to engage in free, uncontrolled, and unlimited access to the Reynolds system for its own profit. Authenticom further touts its own prices as being the correct competitive benchmark—despite the fact that it can charge such prices only by freeloading on Reynolds's system's functionalities and intellectual property. But nothing in the law permits Authenticom to access the Reynolds DMS without permission from Reynolds, the creator, owner, operator, and licensor of the DMS. Nothing in the law requires Reynolds to deal with Authenticom, either. Authenticom is a hacker, one that disguises its thievery in a cleverly pleaded euphemism, claiming it is in the business of providing "data integration"[1] services. Authenticom's real business is system bootlegging: unlawfully logging into the Reynolds DMS, utilizing the system's capabilities to process and report information, and then extracting, repackaging, and selling that information to others.

11. In short, Authenticom's Reynolds-DMS business model relies entirely on unauthorized, unsecure, and illegal access to a proprietary computer system that Reynolds has painstakingly built and protected at extraordinary expense. Authenticom is a software pirate that

[1] Authenticom calls itself a "dealer data integration provider," but it admits it offers "no *actual* 'integration'" services "in the traditional sense"; "[i]nstead, in this context, 'integration' is *simply a synonym for data access*." *Authenticom* Dkt. 4 at ¶¶ 2, 54 n.4 (emphases added).

free-rides on a computer system it has not borne the cost of building, securing, or maintaining. And Reynolds, not Authenticom, will be left holding the bag if and when Authenticom's uncontrolled, unmonitored, and unauthorized access methods and sloppy security practices cause a DMS system crash, data breach, or loss of intellectual property.

12. Every time Authenticom provides its bootleg "integration" services to a dealer who licenses the Reynolds DMS software, it tortiously interferes with Reynolds's contractual relationship with that dealer. Every time Authenticom uses misappropriated login credentials to access the Reynolds DMS without Reynolds's authorization, it fraudulently misrepresents that it is an authorized dealership employee, commits a trespass to chattels under the common law, and violates the federal Computer Fraud and Abuse Act, the Wisconsin Computer Crimes Act, and the California Comprehensive Computer Data Access and Fraud Act. Every time Authenticom runs the Reynolds DMS PC software, it infringes Reynolds's copyrights. Every time Authenticom circumvents Reynolds's security measures that govern access to and copying of material on the DMS, it violates the Digital Millennium Copyright Act. Every time Authenticom succeeds in its unrelenting efforts to command Reynolds DMS servers to run and execute commands at Authenticom's direction, Authenticom has converted those servers. Every time Authenticom accepts payment for its bootleg integration services, it unjustly enriches itself at Reynolds's expense. In short, as it pertains to Authenticom's unauthorized use of the Reynolds DMS system, its business is wholly unlawful. As a result, Authenticom's business model violates the California Unfair Competition Law. Reynolds is entitled to a permanent injunction to compel Authenticom to stop.

13. As a result of its wrongful and illegal actions, Authenticom is liable to pay statutory and common law damages to Reynolds. Reynolds is also entitled to additional equitable relief from

Authenticom in the form of restitution and disgorgement of Authenticom's profits that relied, even in part, on unauthorized and stolen access to the Reynolds systems. Finally, Reynolds is entitled to a permanent injunction barring Authenticom from accessing the Reynolds system without Reynolds's authorization. Paying damages for past injuries, alone, is not enough: Authenticom has alleged its business model depends on its ability to use Reynolds's systems, despite its lack of a license to do so, and so it is overwhelmingly likely that Authenticom will continue to hack the Reynolds system in the future. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

I. PARTIES

14. Counterplaintiff The Reynolds and Reynolds Company is a privately held Ohio corporation with its corporate headquarters and principal place of business at One Reynolds Way, Kettering, Ohio 45430.

15. As alleged in its complaint, Counterdefendant Authenticom, Inc. is a privately held Wisconsin corporation with its corporate headquarters and principal place of business at 400 Main Street, La Crosse, Wisconsin 54601. *Authenticom* Dkt. 4 at ¶ 19.[2]

II. NATURE OF THE COUNTERCLAIMS

16. These counterclaims arise under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; the Copyright Act, 17 U.S.C. § 501; the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201; the Wisconsin Computer Crimes Act ("WCCA"), Wis. Stat. § 943.70(2)(a); the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal

[2] Throughout this complaint, references to the *Authenticom* docket are to the pre-consolidation docket in this case, 3:17-cv-00318-jdp, accessible via the Western District of Wisconsin PACER site.

Code § 502; the California Unfair Competition Law, Cal. Bus. and Prof. Code § 17200; and the common law.

17. This Court has jurisdiction over these counterclaims pursuant to 28 U.S.C. §§ 1331, 1332(a)(1), 1367(a), 2201(a), and 2202. There is federal question jurisdiction under 28 U.S.C. § 1331 because Reynolds seeks to enforce its federal statutory rights under the CFAA, the Copyright Act, and the DMCA. There is diversity jurisdiction under 28 U.S.C. § 1332(a)(1) because Reynolds is a citizen of Ohio, Authenticom is a citizen of Wisconsin, and the amount in controversy with respect to these counterclaims exceeds the sum or value of $75,000, exclusive of interest and costs. There also is supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367(a) because they are so related to claims in the action within the Court's original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

18. This Court has personal jurisdiction over Authenticom because it is located and does business in the District in which this action was filed; because many of its illegal actions challenged in these counterclaims occurred in, and/or were directed from, that District; and because Authenticom filed a complaint against Reynolds in that District.

19. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c).

III. RELEVANT BACKGROUND

a. The Reynolds DMS Is A Complex, Bespoke, Premium Computer System That Contains Highly Sensitive Data and Is Protected by Copyright

i. Reynolds Has Invested Hundreds of Millions of Dollars and Millions of Man-hours to Build the Most Stable, Secure, and Sophisticated Dealer Management System on the Market.

20. Reynolds was founded in 1866 and formally incorporated in Ohio in 1889. It has been partnering with retail automotive dealers to improve their business operations since the

1920s, when Reynolds created the first standardized account forms and a paper-based accounting system for the retail automotive industry.

21. Reynolds introduced "ERA," the first computerized DMS, in the late 1980s. The Reynolds DMS is an integrated, complex system of hardware and software components that enable retail automotive dealers to manage their inventories, customer contacts, financial and insurance information, transactional details, government reporting and compliance requirements, human resources files, and a myriad of other tasks involved in managing an auto dealership. ERA is Reynolds's principal DMS product.

22. In October 2006, following a merger by acquisition, Reynolds and Dealer Computer Services, Inc. ("DCS") merged operations. DCS had developed a separate DMS product in the 1980s. That product is currently known as POWER and continues to be offered under Reynolds's ownership and control. Unless otherwise noted, ERA and POWER will collectively be referred to as "the Reynolds DMS."

23. The Reynolds DMS consists of numerous hardware and software elements. At a very high level, those components include the following:

a. A dealer-side server (either in the form of a standalone server physically on site at the dealership or a cloud-hosted server);

b. An operating system on the server;

c. Multiple databases on the server;

d. Application software on the server;

e. A secured software interface between the server and the dealer's PCs;

f. Terminal and application software on the dealer's PCs;

g. Secure data connections between the dealer-side server and the "Reynolds Integration Hub," and

h. The Reynolds Integration Hub itself, which includes numerous layers of security, monitoring and other proprietary functions designed to, among other things, seamlessly integrate numerous vendors, manufacturers, and others into the DMS ecosystem in a secure, real-time manner.

24. The proprietary design and interaction of these various components reflects Reynolds's decades-long efforts to provide the most stable and secure DMS platform on the market. Reynolds has staked its brand and reputation on providing such a platform, and has invested heavily in building, securing, and maintaining its DMS platform. Over the course of the last two decades, those investments are easily in excess of hundreds of millions of dollars and millions of man-hours.

ii. The Reynolds DMS Does Not Merely Contain "Dealer Data"

25. Authenticom's core thesis in this litigation is that the data on the DMS "belongs to the dealer." As an initial matter, that claim is a fundamental misdirect: the core dispute in this case is about *system* access, not *data* access—as evidenced by the fact that dealers have the ability to export their data from the DMS at will, using a robust and integrated suite of reporting tools (discussed below). Moreover, Authenticom's claim that the data on the DMS "belongs to the dealer" is also materially false. In addition to its many other functions and operations, Reynolds's proprietary system processes and stores not only dealer operational and financial data, but also confidential consumer, automotive original equipment manufacturer, financial institution, and credit bureau information, reference data, and intellectual property owned by Reynolds and other third parties. DMS-processed data includes numerous categories of sensitive "Personally Identifiable Information" or "PII."

26. Reynolds's DMS also processes a related, overlapping category of protected information known as Nonpublic Personal Information ("NPI"). Virtually all of the information that a consumer provides to a dealership constitutes either PII or NPI.

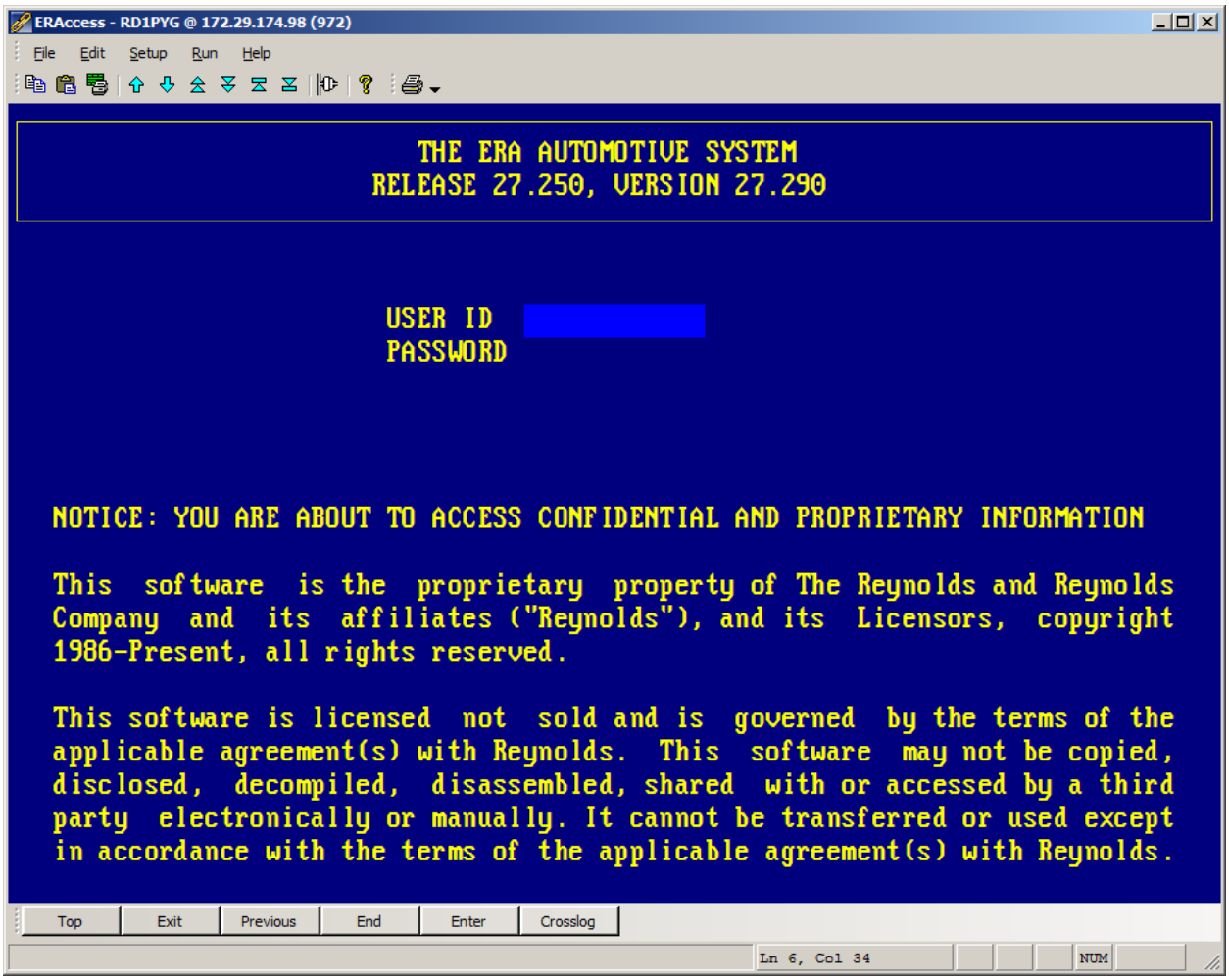
27. In addition, Reynolds's DMS processes and securely stores sensitive information belonging to automotive manufacturers ("OEMs"), such as codes and prices for parts and labor, rebates and incentive information, and warranty information.

28. Reynolds's DMS also processes and securely stores sensitive information belonging to other third parties, such as credit check information generated by Experian and other credit reporting bureaus.

29. In addition, Reynolds's DMS processes, and is largely comprised of, valuable intellectual property. This intellectual property includes, but is not limited to, the software that comprises the DMS itself.

iii. Reynolds's DMS Is Protected by Copyright

30. The Reynolds DMS PC software program that runs on dealer computers is an original copyrighted work. Among the many significant original elements of the program are its source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience. Every time a user opens the DMS PC software program, the program displays a notice that, among other things, clearly and explicitly states that the program is Reynolds's copyrighted, confidential, and proprietary property:



31. As set forth below, it is impossible for a user to access or use the core DMS without running (and thereby copying) Reynolds's copyrighted DMS PC software programs.

32. Authenticom does not now have, nor has it ever had, Reynolds's permission to access or use the DMS to exfiltrate data and sell that data to third parties. Nor has it ever had a valid license or sublicense to do so.

b. Reynolds Invested Heavily in the Reynolds Certified Interface Program to Build a Stable, Secure, Real-Time Data Transfer Platform.

33. As discussed above, Reynolds has staked its brand and reputation on providing the most stable and secure DMS platform on the market. Access to the DMS without Reynolds's

authorization, especially automated access, constitutes a threat to that reputation, to the system, to Reynolds's intellectual property, and to the data stored on the system.

34. At the same time, Reynolds's dealership customers often desire to use various third-party applications as part of their business operations. These include software applications that provide automated license-plate registration, customer relationship management, dealership marketing assistance, information technology, website management, and other services. Other vendors, like TRUECAR, provide vehicle pricing for the dealers' customers using Vehicle Sold information from the dealers' inventories. Such third-party applications often desire to leverage the functionality and contents of the DMS platform.

35. Although many vendors wish to leverage the DMS by pulling processed data out of the DMS platform, some also seek the ability to "push" or "publish" data back into the DMS so that it can populate the DMS's various systems and databases for computation and organization by the system. For example, vendors seeking to amend customer records or input service appointments often desire such write-back abilities to allow that information to interact with the Reynolds systems' other functions.

36. Providing dealers with a managed, functional, and secure method for applications to leverage the functionality and contents of the DMS is a critical part of ensuring that Reynolds's DMS is competitive in the DMS marketplace. Dealers are fully aware of what applications are licensed or authorized to leverage each DMS platform, and DMS providers frequently use applications' compatibility with their system as a point of competition with each other. Reynolds's RCI functionality is accordingly central to Reynolds's business strategy, distribution scheme, and marketing plan.

37. In order to facilitate secure real-time interfaces between the DMS and third-party applications, Reynolds developed technology to support the RCI program. The RCI program facilitates third-party interfaces that allow third parties to leverage the benefits of the DMS while imposing carefully constructed layers of safeguards and protections between the vendors and the DMS itself. It provides application vendors with the ability to both receive and, if appropriate, push data into the DMS via dedicated, customized interfaces. These interfaces are designed to ensure that a vendor receives only what is necessary for the dealer's business needs for that vendor and to minimize the impact of the additional DMS system burden. Reynolds's interface protocols ensure that third parties do not directly access the DMS.

38. As part of its system, Reynolds has built over 1,600 customized interfaces, deployed in over 50,000 custom packages that engage in approximately 260,000,000 data transactions a month. Reynolds employs more than 5,000 people and devotes enormous resources to building, maintaining, and monitoring the DMS and its incorporated interface protocols through its integration hub.

39. Reynolds works with each vendor seeking RCI certification to determine the precise types of interface functionality and data element needs that the vendor requires to operate its application, the specific business rules that will apply to the data, the frequency with which the data needs to be refreshed, and, as appropriate, whether the application needs bidirectional interface functionality. The interfaces are then built, configured, and tested to ensure that the third-party application is appropriately interfacing with the DMS.

40. Reynolds has built numerous safeguards—including redundant layers of hardware and software protection—into the DMS to support system stability. For example, the RIH includes a "journaling" function that protects against the risks inherent in allowing large-scale automated

"write-back" from vendor software into dealer databases. After vendor software performs its particular function, dealers and vendors want the results of that function to be reflected in the Reynolds DMS servers and populated according to the system's proprietary business rules. To take a common example, a dealer using third-party inventory management software would typically want that software to be able to accurately update the number of cars on the lot following a sale. But large-scale automated write-backs, if permitted, come with inherent risk: these automatic data pushes involve far more entries and transactions than an individual human user could produce, and if the vendor software malfunctions, it can produce and push thousands of erroneous data entries in the span of minutes. Those erroneous data entries can have a contagion effect as they propagate across the dealer's system—since many DMS functionalities rely on data streams from other portions of the DMS—potentially paralyzing the dealer's operations.

41. Reynolds's journaling technology—which Reynolds built from the ground up—is a critical backstop that allows Reynolds to unwind the potentially catastrophic effects of malfunctioning vendor software. Journaling minimizes potential down time for dealers and vendors, as well as the risk of DMS data being erroneously overwritten by a vendor.

42. Reynolds's integration protocols, support and monitoring, and the RCI program further ensure that dealers' DMSs are not overloaded as a result of third parties "pinging" the system with constant computer processing requests. The dealer side of the DMS is never pinged or touched by RCI partners. RCI (via the RIH) provides Reynolds with the ability to monitor each vendor's data feed and promptly detect any disruptions or errors in real time. Reynolds's integration technology provides Reynolds with the ability to audit and trace potential security breaches. Reynolds integration technology also protects system stability because its custom interfaces are carefully designed to avoid disrupting critical system updates and tasks.

43. In addition to its own proprietary system security measures, Reynolds also imposes stringent contractual security obligations on its RCI vendor partners in their license and interface agreement. RCI vendors are prohibited from using unapproved methods to access the DMS; are required to notify Reynolds promptly in the event of a security breach; and must warrant to Reynolds that they comply with data security and privacy laws. Moreover, Reynolds requires vendors to include certain terms in their End User License Agreements with dealers. One of these terms requires both the vendor and dealer to implement and maintain safeguards designed to protect sensitive customer information. Reynolds reserves the right to—and frequently does—audit its RCI vendor partners' End User License Agreements to ensure compliance. These contractual requirements for RCI certification protect dealer and consumer data by aligning incentives, and they also give Reynolds an avenue for indemnification in the unlikely event that an RCI partner suffers a data breach.

44. Of course, when Authenticom uses automated software to access, use, and scrape data from the DMS, and then sends that data to unknown and unapproved third parties, Reynolds receives no such assurances. Hostile data scrapers like Authenticom that mask as credentialed dealer-side employee users also bypass *all* of these important safeguards and rob dealers of the system stability and protection they bargained for with a Reynolds DMS.

45. These mission-critical security and stability measures—customized interfaces with carefully limited data access, multilayered hardware and software redundancies, sophisticated journaling, and segregation of vendor system interaction from dealer-side communication with the Reynolds DMS servers—were expensive and difficult to build, and are expensive and difficult to maintain. Just as the Reynolds system is a premium DMS, the RCI program is a premium integration platform. It provides best-in-class stability and security.

c. Reynolds Provides Dealers with Robust Tools to Export Their Data from the DMS.

46. Although automated access is not allowed by either the Reynolds system or the license agreements under which it is offered, Dealers are authorized and able to use the robust reporting functionality built into the system to export operational data as needed. [redacted]

47. Reynolds's ERA DMS contains a functionality called Dynamic Reporting. This reporting tool allows dealership employees to build customized reports—i.e., data exports from the DMS—with extensive flexibility. Dynamic Reporting reports can be scheduled to run at any time automatically, up to four times a day. They can also be run manually by a dealership employee at any time. Dealers can then send or push to the third party, or allow the third party access to a PC where the downloaded data is housed. (POWER contains analogous features, although there are some technical differences.) Previous versions of the Reynolds DMS also contained similar (though less advanced) reporting tools called Report Generator and Query Builder.

48. In addition, Reynolds offers a program called AVID—"Automated Vehicle Inventory Downloads"—by which Reynolds has configured an automated report for third parties to retrieve vehicle-inventory data. The AVID process pushes the vehicle-inventory data to a secure destination (at the dealership or to Reynolds), where dealers can arrange for third parties to retrieve it. In addition, Reynolds provides dealers with several data transfer options related to their banking and payroll functions, including positive pay and direct deposit.

49. Reynolds's clearly articulated and widely publicized policy for ***over a decade*** has been that, outside of the options noted above, "all third-party vendors that want data from a dealership's Reynolds system [must] be certified through the Reynolds Certified Interface program or receive the data via a download from Dynamic Reporting." *Authenticom* Dkt. 71-8 (Nemelka Decl. Ex. 33). Reynolds has not been secretive about these policies, but rather has been the industry leader in requiring certified interfaces with its system as "the safest way to protect [dealer] data … while still supporting the need for moving data to third parties and OEMs." *Authenticom* Dkt. 71-7 (Nemelka Decl. Ex. 32); *see also Authenticom* Dkt. 70-21 (Nemelka Decl. Ex. 21). Reynolds maintains that utilizing certified interfaces is the best way to transfer data—particularly of a sensitive nature—but at the end of the day, Reynolds's dealership customers are free to take all of their operational data out of the DMS and send it to Authenticom (or others) whenever they want, subject only to their own independent legal, regulatory, and ethical obligations.

d. Reynolds Has Secured its DMS System with a Series of Safeguards Designed to Thwart Unauthorized Access, Use, and Copying.

50. Because the Reynolds DMS is critical to business operations and includes commercially valuable intellectual property and critically sensitive data belonging to Reynolds, automobile manufacturers, dealers, and dealership customers, Reynolds carefully controls access to the DMS platform to maintain robust system stability and functionality, prevent unauthorized use, and guard data security.

51. Access to the DMS by a dealership is controlled through a series of security measures, beginning with a login prompt that requires a user to enter a valid username and password to use the system. After a user has successfully logged in, the user encounters a series of visible and invisible security measures in the course of accessing and using different parts of the Reynolds DMS.

52. For example, users who want to use the DMS's data exporting functions must pass through a CAPTCHA control. The test consists of a word or series of letters and numbers that have been stretched and twisted, typically displayed against a color-gradient background. Because humans and computers process and recognize patterns differently, humans can easily pass CAPTCHA controls, whereas bots and similar automated scripts encounter difficulties. It is impossible for a dealer user to access these and other portions of the Reynolds DMS platform without passing a CAPTCHA control.

53. A suite of invisible access controls also helps secure the Reynolds DMS from would-be hackers. For example, Reynolds's Suspicious User ID monitoring software monitors a variety of factors that differentiate automated scripts and bots from bona fide human users, including but not limited to keystroke speed, keystroke pattern, and the volume and timing of data requests. When the software determines that users are suspicious, based on a combination of the factors it monitors, the system protocols flag that user ID for deactivation. These system controls are agnostic as to the identity of the would-be hacker and are automatic.

e. Reynolds's Licensing Agreements Explicitly Prohibit Dealers from Allowing Third Parties Like Authenticom to Access and Use the DMS System.

54. Reynolds licenses its DMS to dealerships pursuant to the Reynolds Customer Agreement, which is a licensing agreement that grants [redacted]

55. Authenticom has admitted in its own proposed findings of fact at the preliminary injunction hearing that Reynolds's contracts categorically prohibit dealers from giving access to the DMS to "any third party." *Authenticom* Dkt. 63 at ¶ 153; *see also Authenticom* Dkt. 65-24 § 1

(Nemelka Decl. Ex. 49).

[redacted]

58. [redacted]

59. [redacted]

60. [redacted]

61. Authenticom is, and at all times relevant to the claims at issue in this suit has been, aware of these restrictions. The fact that Reynolds imposes these contractual licensing restrictions has been widely known in the automotive industry for more than a decade, as has the fact that Reynolds actively enforces the restrictions, both legally and technologically. Authenticom's own complaint cites *Automotive News* articles proclaiming these policies in 2006-2008.

62. In 2013, the United States District Court for the Southern District of Ohio further recognized Reynolds's licensing restrictions in dismissing another putative integrator's antitrust claims against Reynolds in a public order, stating:

> Reynolds' auto-dealership customers agree to certain prohibitions on integration of third party applications when the customers license Reynolds' ERA. When they sign up for ERA, customers typically agree to prohibitions on connecting third-party applications to ERA. The customers also agree to prohibitions on allowing third-party integrators that are not licensed by Reynolds, like SIS, to interface with ERA.

Reynolds & Reynolds Co. v. Superior Integrated Sols., Inc., 1:12-CV-848, 2013 WL 2456093, at *2 (S.D. Ohio June 6, 2013) (citations omitted).

63. On the stand, Authenticom's founder and president, Stephen M. Cottrell attempted to equivocate on the issue of whether he was aware of the restrictions, stating that "there were lots of things that had been said" and "lots of talk in the marketplace" about the Reynolds license's controls on dealer's ability to allow third parties to access and use the Reynolds DMS. *Authenticom* Dkt. 162 (6/26/17 Afternoon Session Tr. at 19:11-16). But later, Authenticom produced documents clearly indicating that it was in fact provided copies of the specific language in Reynolds's licensing agreements prohibiting its access. To the extent there could have been any doubt about Reynolds's policy (there couldn't have been), Mr. Cottrell actually received a copy of the contractual restrictions in 2015 in connection with Reynolds's continued demands that Authenticom cease and desist from its illegal activity. Ultimately, Mr. Cottrell testified that he

was aware of the exact language prohibiting dealers from giving Authenticom login credentials as of the first quarter of 2015. *Id.* at 18:17.

64. These licensing restrictions are a core aspect of Reynolds's business strategy, distribution scheme, and marketing plan. Reynolds is in the business of building and licensing a robust computer software and hardware ecosystem, and its controls on access to and use of that environment are absolutely central to its ability to control, operate, maintain, monitor, and secure its proprietary DMS platform.

65. Some dealers disagree with these prohibitions on third party and automated access, while others appreciate and affirmatively agree with them. Dealers who disapprove of the restrictions are free to switch from Reynolds to other DMS providers that follow less stringent data security practices (or decline to use Reynolds in the first place) as a result of these contractual requirements. In fact, many dealers have switched to other DMS providers' more "open" systems. At the same time, numerous other dealers have either switched or returned to Reynolds because they prefer the stability, security, and other premium features that its DMS provides.

66. One of Authenticom's counsel's other clients in this MDL – Cox Automotive – specifically commissioned a study by "partner[ing] with two independent research firms to conduct studies with hundreds of dealer respondents." According to Cox's public statements about this report, at contract renewal 45% of small groups, 31% of medium sized groups, and 21% of large groups switched at their last renewal date. Switching is common. Dealers have a choice of DMS providers, and Reynolds offers a stable, robust option to sophisticated dealers that is premised, at its core, on a controlled computing environment.

f. For Years, Authenticom Has Relentlessly Hacked the Reynolds DMS in Order to Sell Data to Unknown Third Parties, Placing Critically Sensitive Data at Risk and Compromising System Functionality.

67. In order to facilitate its cut-rate bootlegging, Authenticom induces dealers to violate their Reynolds license agreements by sharing existing login credentials or creating new ones for Authenticom to use, then allowing Authenticom's hostile bots to access and use the system, as Mr. Cottrell testified at the preliminary injunction hearing. *Authenticom* Dkt. 164 (6/26/17 Morning Session Tr. 108:4-7). Authenticom then sells the fruits of this unauthorized hoovering to other outside parties.

68. Reynolds has put Authenticom on notice that its "brazen" attempts to gain "unauthorized access" to Reynolds's DMS are "contrary to Reynolds's security policies, compromise[] the operational integrity of Reynolds's system and, perhaps most importantly, violate[] the agreements that Reynolds enters into with its dealership customers." *Authenticom* Dkt. 72-7 (Nemelka Decl. Ex. 57). For its part, following the Court's dismissal of its unsupportable exclusive dealing claim aimed at the Reynolds dealer licensing agreements, Authenticom elected not to challenge these agreements. In other words, the contractual restrictions on dealers sharing credentials to Reynolds's proprietary system are *not* challenged Reynolds conduct.

69. Reynolds unequivocally has demanded that Authenticom "cease and desist from accessing Reynolds's proprietary software and hardware without the proper license and authorization to do so." *Id.* Authenticom admits, as it must, that Reynolds repeatedly has objected to Authenticom's actions as constituting tortious interference with Reynolds's dealer and vendor contracts. *See Authenticom* Dkt. 69 at ¶ 188-89.

i. Authenticom Knowingly Induces Dealers to Breach Their License Agreements by Providing Authenticom With Reynolds DMS Login Credentials

70. In its complaint, Authenticom admits that it repeatedly has used its improperly-obtained credentials to "bridge" into the Reynolds DMS without Reynolds's permission or authorization and, using "user emulation" software, "pull[ed]," "extract[ed]," and "scrape[d]" data from within the Reynolds DMS for sale to third-party vendors and "'push[ed]' data back into the DMS database" in altered form. *Authenticom* Dkt. 4 at ¶¶ 50, 54-55 & n.4, 77-80. Indeed, Mr. Cottrell has bragged that his company gives vendors a "pipeline into [Reynolds] dealerships." But this "pipeline" is really a series of brazen and illegal hacks. The centerpiece of Authenticom's hacking efforts is an automated program that uses unauthorized and unlawful means to log into the proprietary Reynolds DMS, bypass or break through critical security and access controls, and execute Reynolds's proprietary, copyrighted software to suck data out of the DMS. *Authenticom* Dkt. 104-22 at 9 (Gulley Decl. Ex. 66). Through this chosen business model, Authenticom has trampled on Reynolds's contractual and intellectual property rights, trespassed on Reynolds's servers, created significant impairments and risks of harm to both Reynolds's DMS and its customers, and profited on the back of Reynolds's significant investment.

ii. Authenticom Repeatedly And Persistently Circumvents Reynolds's DMS Access Controls

71. Reynolds has backed its objections up with continuing efforts to protect the DMS, including through continuous modifications and improvements to the security measures described above. Authenticom admits that, since at least 2009, Reynolds has been "disabling," "disrupting," and "blocking" Authenticom's unauthorized efforts to get inside Reynolds's DMS. *Authenticom* Dkt. 69 at ¶¶ 109-12, 137, 191. Indeed, according to Mr. Cottrell, Reynolds undertook "intensified" blocking efforts in 2013 that "resulted in an almost complete collapse of Authenticom's integration business for dealers using the Reynolds DMS." *Authenticom* Dkt. 62 at ¶ 38.

72. One auto industry analyst has likened the situation to a game of "Whack-A-Mole": "Vendors get shut out, and then find a way to work around the problem by finding a 'hostile' or backdoor entry. Reynolds then finds the backdoor entry and shuts it down." *Authenticom* Dkt. 71-14 (Nemelka Decl. Ex. 39). Every time Reynolds puts an access control in place, Authenticom attempts—sometimes successfully—to hack around the control.

73. [redacted]

74. [redacted]

75. [redacted]

76. Similarly, Authenticom has consistently adapted its "user emulation" software to avoid Reynolds's Suspicious User ID monitoring software. Reynolds does not know the details of how Authenticom has modified the program to avoid Suspicious User ID detection, but Authenticom has engaged in a persistent campaign to circumvent this protection measure since Reynolds first introduced it in 2013.

77. Authenticom's own complaint states that, in response to Reynolds's longstanding efforts to prevent Authenticom and others from hacking into the Reynolds DMS, Authenticom has attempted for years to "navigate around" Reynolds's "blocking efforts"—i.e., hack around the security measures discussed above, including login controls, CAPTCHAs, and the Suspicious User ID detection software—through various "workaround solutions," including "user emulation" (i.e., falsely representing to be dealers logging into their own DMS accounts). Compl. ¶¶ 55, 195.

78. According to its preliminary injunction briefing, Authenticom "worked with dealers to develop workaround solutions that circumvented Reynolds'[s] efforts to block access" to the Reynolds DMS. *Authenticom* Dkt. 67 at 8.

79. Despite Reynolds's best efforts, Authenticom's circumvention efforts were often successful, and it repeatedly accessed the Reynolds DMS after disabling, bypassing, or evading the various security measures Reynolds had in place. The above citations to Authenticom's pleadings, briefing, documents, and testimony make clear that Authenticom circumvented Reynolds's access controls as a matter of routine. Authenticom's document production since then leaves no doubt: Authenticom's business model with respect to Reynolds was to hack around Reynolds system security.

80. Authenticom even advertises its ability to circumvent Reynolds's access control measures, at one point publicly vowing to continue to hack its way into the DMS "*despite whatever*

hurdles are placed in our path."[3] Authenticom has repeatedly emphasized its ability and intent to, in Mr. Cottrell's euphemistic phrasing, "navigate around the shutdowns." *Authenticom* Dkt. 62 at ¶¶ 40-41; *see also Authenticom* Dkt. 69 at ¶¶ 210-11.

g. Authenticom Has Made Countless Copies of Reynolds's Copyrighted Software, Without Any Valid License or Sublicense

81. After bypassing the login and other access controls, Authenticom's bots run the Reynolds DMS PC software program using automated scripts that "emulate" a dealership employee's use of the system. *Id.* at 108:15-19. Every time Authenticom accesses and runs the Reynolds DMS PC software, it creates a copy of the copyrighted DMS PC software program code in the computer's Random Access Memory.

82. [redacted]

h. Authenticom's Actions Have Caused Extensive, Ongoing, and Irreparable Harm to Reynolds, While Furthermore Imperiling Reynolds, Dealers, and Consumers

83. Authenticom's relentless efforts to hack into Reynolds's DMS and to "scrape" and "extract" information out of the Reynolds DMS without Reynolds's permission have caused a variety of serious and ongoing injuries to Reynolds and its dealers. In addition to the threat posed

[3] Stephen Cottrell, *Why Certification?* (Authenticom public letter dated June 2015), *available at* https://web.archive.org/web/20160418122902/http://www.authenticom.com/pdf-downloads/Why%20Certification.pdf (Wayback Machine internet archive snapshot from April 18, 2016, last visited February 20, 2018).

to the integrity and functionality of the Reynolds DMS itself, Authenticom has put at risk automotive manufacturers, credit bureaus, financial institutions, and, most importantly, millions of people whose PII and other confidential data are jeopardized by Authenticom's casual approach to cybersecurity.

84. Hostile integrators like Authenticom are a cyber-security "black hole"—a catastrophic data breach just waiting to happen. Authenticom's hacking and unauthorized access practices violate widely accepted cybersecurity practices and directly contradict guidance from the National Automotive Dealers Association.

85. Authenticom bypasses all of the interfaces, protections, and resources that Reynolds has built into its dedicated integration hub by accessing the system as a purported individual employee user with illegally obtained employee credentials. Authenticom instructs Reynolds's DMS licensees to configure access credentials for Authenticom's use with access set to "Grant Access to All Data Sets in All Run Areas" (the broadest DMS access setting for employee users) and then directly accesses the DMS through these pirated log-in credentials—as though it was an authorized dealership employee. This employee user-access setting enables a user to access substantially all of the data on the DMS available to the most-trusted dealership employee, regardless of the scope of work that Authenticom is meant to provide for the dealer or for the third-party software applications that are paying Authenticom. Given that configuration, Authenticom's assertion that it only accesses the narrow category of information that the vendor requires and the dealer authorizes is flatly untrue. And given the indiscriminate character of Authenticom's data collection techniques—screen scraping and bulk automated downloads—Authenticom's more limited assertion that it only *copies* the fields that vendors require and dealers authorize is almost certainly false.

86. Moreover, although bootleggers like Authenticom seek to imitate real time access like that provided by RCI, they cannot do so. Genuine real-time access is available only from the system provider. (That's why application providers that want true real-time access pay an "open" system provider like Cox more for system integration (i.e., "OpenTrack"), even though Cox also authorizes non-integrated, third-party access like Authenticom's).

87. Instead of the real-time data transfer that RCI offers, Authenticom accesses the system from the *dealer side* (designed for and licensed for use by only human dealership employees) with thousands of automated transactions to scrape information, causing system load and harming stability and system performance. All the while, Authenticom bypasses the critical central safeguards of Reynolds's integration technology (which was designed and built precisely to securely and efficiently handle automated commercial integration for specific commercial users). Put simply, *any* unauthorized, uncontrolled access threatens the Reynolds DMS (as it would any computer system or network). Indeed, from Reynolds's perspective, Authenticom's access attempts and methods are indistinguishable from a hostile hacker. That is why Reynolds and other computer system operators go to extraordinary lengths to prophylactically detect and block unauthorized and uncontrolled access.

88. Authenticom's position on cybersecurity appears to be: "Trust us." But Authenticom does not appear to be especially trustworthy when it comes to its data security practices. Authenticom's cavalier attitude toward cybersecurity is best summarized by reference to Mr. Cottrell's testimony at the preliminary injunction hearing.

89. Cross-examination revealed that Mr. Cottrell falsely represented to the court that Authenticom had for three years received a Microsoft "gold security certification"—a certification that does not exist. *Compare Authenticom* Dkt. 62 at ¶ 31 *with Authenticom* Dkt. 162 (6/26/2017

Afternoon Session Tr. at 25:15-26:10). In any event, Microsoft itself is clear that simply being a customer of its Azure storage platform does not ensure Authenticom is secure or obviate Authenticom's many security obligations.[4] Indeed, the highly publicized recent data breach at Deloitte occurred on the same Microsoft Azure platform that Authenticom has touted.[5]

90. Cross-examination also suggests that, whatever the sincerity of Mr. Cottrell's professed passion for security, he is woefully uninformed about cybersecurity developments, not only in his own market segment but as regards his own data transfer partners. In August 2016, the cybersecurity press broke news that DealerBuilt—a competitor DMS—had suffered a serious data breach incident that resulted in millions of individuals' confidential information being leaked online. Dfts. P.I. Ex. 151.[6] At the June 2017 hearing (over ten months later) Mr. Cottrell testified that he "just recently learned" of the DealerBuilt breach, *despite the fact that Authenticom has a data transfer agreement with DealerBuilt*. *Authenticom* Dkt. 162 (6/26/2017 Afternoon Session Tr. at 22:1-6). This bears repeating: Authenticom's CEO and President was unaware, for nearly ten months, of a massive data breach that affected his own data transfer partner.

91. Authenticom, itself, uses methods known to pose cybersecurity risks, including apparently using hardcoded credentials and poor security practices that allow plaintext credentials to its servers to be found on the Internet.

92. Incredibly, Mr. Cottrell testified that, in his opinion, DMSs are "not a high value target" and so he did not think it was likely that hackers would target them. *Id.* at 23:2-5.

---

[4] *See* Frank Simorjay, *Shared Responsibilities for Cloud Computing* at 5 (Microsoft White Paper, April 2017), *available at* https://perma.cc/3D2Q-TCPH.

[5] *See, e.g.*, Nick Hopkins, *Deloitte hit by cyber-attack revealing clients' secret emails*, The Guardian (Sep. 25, 2017), *available at* https://perma.cc/7PVL-3FS3.

[6] *See also* Zack Whittaker, *Bought a Car Recently? Millions of dealership customer details found online*, ZDNet (Nov. 8, 2016), *available at* http://www.zdnet.com/article/bought-a-car-recently-millions-of-customers-records-found-online/ [https://perma.cc/4K85-8GQN].

93. This blasé attitude toward the security of the highly sensitive information stored on the DMS infects Authenticom's cybersecurity practices from root to branch. For example, Authenticom regularly communicates confidential DMS login credentials over the telephone and via unencrypted clear text in email or web forms. Per Authenticom's configuration instructions described above, these credentials—transmitted "in the clear"—have access to *substantially all of the information on the DMS* and are harvested by Authenticom *for the express purpose* of creating an outside "*pipeline*" to the DMS (in Mr. Cottrell's words). This is all before the information is stored by DealerVault (or Azure) and before it is sold and *retransferred* to other third parties (to possibly be re-retransferred by them).

94. Moreover, based on information received in discovery and otherwise, it is apparent that Authenticom's network and infrastructure security is poor at best. Authenticom has already produced one report indicating that it was subject to a malware infection, and it is highly likely that discovery will expose other vulnerabilities and network breaches. These vulnerabilities would allow hackers to penetrate Authenticom's lackluster cybersecurity measures and access and copy the sensitive consumer, dealer, and institutional data that Authenticom purloined from the Reynolds DMS—as well as potentially Authenticom's pool of improperly-obtained Reynolds DMS credentials. In other words, after Authenticom hacks into and steals data from the Reynolds DMS, it stores that data in an unsecure location where it is vulnerable to be stolen once again by other, still less scrupulous hackers.

95. Even if Authenticom was solid and reliable on data security (and it is not), the basic structure of its business is contrary to elementary cybersecurity principles. Reynolds carefully assesses its RCI partners and requires them to agree to strict security and indemnity provisions, because Reynolds is at risk in data breach and system crash scenarios. Reynolds, moreover,

supports the RCI vendors and assures vendor application functionality through regular updates and other system software protocols and enhancements. This seamless integration and interoperation between third-party applications and the Reynolds DMS is an important part of Reynolds's efforts to differentiate itself in the marketplace.

96. Authenticom has no such incentives and imposes no such requirements. Authenticom does not care about the burdens on Reynolds system caused by its stolen access. When Authenticom hacks the DMS and sends siphoned data to itself and resells it on to third-party vendors, Reynolds has no control over, and no way to know, what data is taken, what data has been corrupted, what computing resources have been used or deployed, or to whom any of the "scraped" data is sent (or resent). Reynolds does not get a say, and Reynolds has no way of knowing whether the vendor on the other end of the transaction is a legitimate and reputable business with strong cybersecurity practices. If a data breach occurs at Authenticom or one of its data buyers, Authenticom's actions impair Reynolds's ability to investigate, trace the source of the breach, remedy the breach, correctly apportion fault/liability, and so forth. Similarly, Reynolds has no forewarning of the burdens to the Reynolds ecosystem or dealer-specific licensed resources imposed by Authenticom's bootleg access. And if Authenticom imposes any meaningful security screening in its selection of third-party vendor partners, that screening process has not been aired in this suit despite strenuous litigation of the adequacy of Authenticom's security practices at the preliminary injunction stage.

97. Authenticom's lax security practices increase the risk that Reynolds will suffer a system crash or data breach. But even if Authenticom was a paragon of data security, it *still* could not, given its hostile (and freeloading) access, be in a position to coordinate system access with

Reynolds to avoid unnecessary functionality problems caused by unauthorized (and unknown/unmonitored) access to the DMS.

98. Additionally, damages in data breach cases far exceed Authenticom's ability to indemnify Reynolds if Authenticom's sloppy security practices are the cause of the breach. Authenticom itself claims to be in dire financial straits, and its $20 million cybersecurity insurance policy—which apparently provides zero coverage to Reynolds—is woefully inadequate. Following their respective data breach incidents, Home Depot has paid out more than $150 million,[7] and Target more than $200 million.[8] The Reynolds DMS processes, secures, and contains far more sensitive consumer information than the breached Home Depot and Target systems, making it an attractive target for cybercriminals. There is no meaningful possibility that Authenticom could remedy the harm of a Reynolds DMS data breach.

99. Setting aside the catastrophic data security risks posed by Authenticom's access to the DMS, that access also compromises core DMS stability and functionality. The very technical measures that Authenticom calls "anticompetitive blocking" are precisely the same defenses that keep out malicious hackers. Moreover, the automated scripts that Authenticom uses "ping" the DMS with computing requests at a rate of hundreds or thousands of times per day are likewise dangerous to the DMS. That speed and volume taxes the computational and network resources of the Reynolds DMS, resulting in degradation of service for dealers and increased operational costs to Reynolds.

100. Since the early 2000s, Reynolds has experienced many incidents where third parties' actions have impaired or even crippled the ability of the Reynolds DMS to function

[7] Jeff John Roberts, *Home Depot to Pay Banks $25 Million in Data Breach Settlement*, Fortune Magazine (March 9, 2017), *available at* http://fortune.com/2017/03/09/home-depot-data-breach-banks/ [https://perma.cc/H5A8-XAP6].
[8] Reuters, *Target Pays Millions to Settle State Data Breach Lawsuits*, Fortune Magazine (May 23, 2017), *available at* http://fortune.com/2017/05/23/target-settlement-data-breach-lawsuits/ [https://perma.cc/PP9R-HQVA].

properly. That, in turn, has caused significant harm to Reynolds's reputation and customer satisfaction with dealers—many of whom did not know or care about the underlying causes but simply saw that their Reynolds DMS was not working.

101. It has been expensive and burdensome for Reynolds to respond to Authenticom's continuing technological gamesmanship and "Whack-A-Mole" tactics. Reynolds has had to invest significant resources in investigating and resolving hostile integration problems caused by Authenticom—a cost that Reynolds alone has had to bear, rather than dealers, third parties, or Authenticom itself. And whenever Authenticom or another hostile integrator succeeds in circumventing all of the dedicated safeguards and resources that Reynolds has built into its system, Reynolds must devote even more resources to counteracting these breaches and attempting to prevent recurrences.

FIRST COUNTERCLAIM FOR RELIEF
(Violations of the Computer Fraud and Abuse Act)

102. Reynolds restates and incorporates all preceding paragraphs by reference.

103. The Computer Fraud and Abuse Act ("CFAA") provides that "[w]hoever … intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer," is subject both to criminal and civil liability. 18 U.S.C. § 1030(a)(2)(C); *see also id.* § 1030(c) (criminal penalties); *id.* § 1030(g) (civil damages and injunctive relief). The CFAA provides for a private cause of action for "compensatory damages and injunctive relief or other equitable relief" to anyone who suffers at least $5,000 in damage or loss in any one-year period "by reason of a violation" of its terms. *Id.* § 1030(g); *see id.* § 1030(c)(4)(A)(i)(I).

104. Reynolds's DMS is a "computer" within the meaning of the CFAA, which defines that term to include not only computing devices themselves but also "any data storage facility or

communications facility directly related to or operating in conjunction with such device." *Id.* § 1030(e)(1). Reynolds's DMS also is a "protected computer" within the meaning of the CFAA because it is used in and affects interstate and foreign commerce and communications. *See id.* § 1030(e)(2)(B).

105. As set forth above Authenticom has repeatedly and intentionally accessed the Reynolds DMS without Reynolds's authorization.

106. Reynolds's Customer Agreements prohibit Reynolds's dealer customers from granting third-party integrators like Authenticom access to the Reynolds DMS without Reynolds's consent. Authenticom has known of these explicit prohibitions for many years and has no reasonable grounds to believe that Reynolds's dealer customers can grant Authenticom access to the DMS on their own.

107. Reynolds's prohibition on Authenticom's access to the DMS is not disputed in this case. Authenticom's challenge to the alleged "exclusive dealing" provisions in these contracts was previously dismissed by this Court, and Authenticom has not repleaded them. Reynolds's dealer contract prohibition on non-employee third party access are not in dispute and Reynolds's prohibitions on this access are not "challenged conduct" in this case. Reynolds's claim against Authenticom for violations of the CFAA is "independent" of any conduct challenged by Authenticom under the antitrust laws.

108. Reynolds has demanded that Authenticom "cease and desist" from accessing Reynolds's proprietary software and hardware without the proper license and authorization to do so, but Authenticom has deliberately disregarded those demands and refused to stop.

109. Instead, Authenticom has repeatedly and intentionally used the information it has obtained through its unauthorized access to the Reynolds DMS in connection with the hostile access services they sell to third-party vendors.

110. Authenticom has caused Reynolds substantial damages and losses, including damages and losses well in excess of $5,000 within the requisite 12-month period. These damages and losses include the costs of investigating and responding to Authenticom's unlawful actions; the costs of restoring the Reynolds DMS and the processed data it contains to their condition prior to Authenticom's unlawful actions; and all revenue lost, costs incurred, and other consequential damages incurred because of disruption of service caused by Authenticom's unauthorized access.

111. Authenticom's violations of the CFAA continue today and will continue into the future if not enjoined by this Court. Authenticom's violations have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

112. Furthermore, Reynolds is entitled to equitable relief in the form of restitution for the benefits that it conferred on Authenticom in the form of uncompensated, illegal access to the Reynolds DMS, or disgorgement of the profits that Authenticom earned through its unauthorized and illegal access.

SECOND COUNTERCLAIM FOR RELIEF
(Copyright Infringement)

113. Reynolds restates and incorporates all preceding paragraphs by reference.

114. The Reynolds DMS and its incorporated works are subject to copyright protection.

115. Reynolds has registered copyrights for multiple versions of the Reynolds DMS PC software program. (Registration Nos. TX 7-586-896; TX 7-586-863; TX 8-538-825; and TX 8-538-541).

116. These programs are original creative works, with distinctive features including but not limited to their source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience.

117. Authenticom admits that it regularly runs the DMS PC software program on dealer PCs through use of its "user emulation" software. *Authenticom* Dkt. 67 at 6.

118. Every time Authenticom runs the DMS PC software program on a dealer PC, it creates a new fixed copy of the DMS PC software program's code in the computer's Random Access Memory.

119. Every time Authenticom "screen scrapes" the Reynolds DMS, it creates fixed copies of Reynolds's original screen layouts, graphical content, and text.

120. [redacted]

121. [redacted]

[redacted]

122. Authenticom's infringement has caused Reynolds substantial harms. Every time Authenticom runs and uses the DMS PC software program, it has, in effect, stolen a license to use the DMS software.

123. Authenticom's infringement will continue into the future if not enjoined by this Court. Authenticom's infringement has wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

THIRD COUNTERCLAIM FOR RELIEF
(Violations of the Digital Millennium Copyright Act)

124. Reynolds restates and incorporates all preceding paragraphs by reference.

125. The Digital Millennium Copyright Act, 17 U.S.C. § 1201, creates three causes of action. The first, Section 1201(a)(1)(A), provides that no "person shall circumvent a technological measure that effectively controls access to a work protected under this title."

126. Section 1201(a)(2) reinforces that direct prohibition by providing that:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with

> that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

127. Section 1201(b)(1) prohibits trafficking in technology that facilitates circumvention of anticopying measures:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;
>
> (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

128. The Reynolds DMS PC software program is an original creative work protected under Title 17. Among the many significant original elements of the program are its source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience. The application software on the dealer PC and on the DMS server that is accessed by the DMS PC software program are also original creative works protected under Title 17. Among the many significant original elements of these programs are their source and object code; distinctive page layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience.

129. Access to, and copying of, the Reynolds DMS PC software program and DMS application software is controlled by numerous technological measures, including passwords, CAPTCHA controls, and Suspicious User ID monitoring. These measures effectively control

access to the DMS PC software program code, as well as the distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience created when the code is executed. In the ordinary course of their operation, the password controls, CAPTCHAs, and Suspicious User ID monitoring software require application of information, or a process or treatment, with Reynolds's authority as the owner of the copyrighted system, to gain access to the program or to certain portions of the program. Authenticom's papers repeatedly admit that these access control measures were effective in preventing Authenticom and other bootleg integrators from accessing the DMS system. *E.g.*, *Authenticom* Dkt. 62 at ¶¶ 37-41; *Authenticom* Dkt. 4 at ¶¶ 106, 189, 195; *Authenticom* Dkt. 67 at 15-17; *Authenticom* Dkt. 162 (6/26/17 Afternoon Session Tr. at 21:11-13).

130. Authenticom has repeatedly bypassed, avoided, disabled, deactivated, or impaired Reynolds's effective access control measures by misappropriating login credentials, hacking through CAPTCHAs, and evading the Suspicious User ID detection program. Indeed, Authenticom represented as much to the court, stating that it routinely and successfully "worked with dealers to develop workaround solutions that circumvented Reynolds'[s] efforts to block access" to the Reynolds DMS PC software. *Authenticom* Dkt. 67 at 8. Authenticom has therefore violated Section 1201(a)(1)(A)'s prohibition on circumvention of a technological measure that effectively controls access to a work protected under Title 17.

131. Authenticom offers a service to the public, a part of which is primarily designed or produced for use in circumventing the access and anticopying controls on the Reynolds DMS PC software program. For example, portions of Authenticom's "user emulation" software are designed and produced primarily for the purpose of bypassing Reynolds's password controls,

CAPTCHA controls, and Suspicious User ID detection software. Authenticom has therefore violated Sections 1201(a)(2) and 1201(b)(1).

132. Authenticom offers a service to the public, a part of which has limited commercially significant purpose or use other than circumventing the access and anticopying controls on the Reynolds DMS PC software. For example, portions of Authenticom's "user emulation" software have no commercially significant use other than bypassing the specific password controls, CAPTCHA controls, and Suspicious User ID detection software that Reynolds uses to secure its DMS platform. Authenticom has therefore violated Sections 1201(a)(2) and 1201(b)(1).

133. Authenticom offers a service to the public, a part of which Authenticom markets for use in circumventing the access and anticopying controls on the Reynolds DMS PC software. For example, Authenticom proudly declared to the dealer consumer base that it will continue to offer its bootleg data integration services "despite whatever hurdles"—that is to say, Reynolds and CDK's security measures—"are placed in our path."[9] Moreover, Authenticom states that it "*worked with dealers* to develop workaround solutions that circumvented Reynolds'[s] efforts to block access[,]" thus using its ability to circumvent Reynolds's access and anticopying controls as an inducement to retain customers. *Authenticom* Dkt. 67 at 8. Authenticom has therefore violated Sections 1201(a)(2) and 1201(b)(1).

134. 17 U.S.C. § 1203(a) authorizes civil actions to remedy violations of §1201. Under § 1203(c)(1), Reynolds has the right to elect either of two damages measures—actual damages plus disgorgement, or statutory damages—at any time before final judgment.

[9]Stephen Cottrell, *Why Certification* (public letter dated June 2015), *available at* https://web.archive.org/web/20160418122902/http://www.authenticom.com/pdf-downloads/Why%20Certification.pdf (Wayback Machine internet archive snapshot from April 18, 2016, last visited February 20, 2018).

135. Further, Section 1203(b)(1) provides that the court "may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation." Authenticom's DMCA violations will continue into the future if not enjoined by this Court. Authenticom's violations have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

FOURTH COUNTERCLAIM FOR RELIEF
(Violations of the Wisconsin Computer Crimes Act)

136. Reynolds restates and incorporates all preceding paragraphs by reference.

137. The Wisconsin Computer Crimes Act ("WCCA") prohibits "willfully, knowingly and without authorization" (1) accessing, taking possession of, or copying "computer programs or supporting documentation"; or (2) disclosing "restricted access codes or other restricted access information to unauthorized persons." Wis. Stat. § 943.70(2)(a). The WCCA provides that "[a]ny aggrieved party may sue for injunctive relief … to compel compliance with this section." *Id.* § 943.70(5).

138. Reynolds's DMS is a "computer program" within the meaning of the WCCA, which defines that term to include not just computing devices themselves, but also "all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer in a computer system or computer network." Wis. Stat. § 943.70(1)(am).

139. Authenticom repeatedly has, including in Wisconsin, "willfully, knowingly and without authorization" accessed, taken possession of, and/or copied the Reynolds DMS and programs and data within the DMS. As set forth above, Authenticom has known for many years that Reynolds's dealer customers are contractually forbidden from giving Authenticom access to the DMS without Reynolds's consent, and Authenticom never has had reasonable grounds to believe otherwise.

140. Reynolds is an "aggrieved party" within the meaning of the WCCA because it is the owner and operator of the DMS that Authenticom has illegally accessed; because Authenticom has tortiously interfered with Reynolds's contractual relationships with its dealer customers; because Authenticom has unjustly enriched itself at Reynolds's expense; and because Authenticom has caused Reynolds various other damages and losses as set forth in these Counterclaims.

141. Authenticom's violations of the WCCA continue today and will continue into the future if not enjoined by this Court. Authenticom's violations have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

FIFTH COUNTERCLAIM FOR RELIEF
(Violations of the California Comprehensive Computer Data Access and Fraud Act)

142. Reynolds restates and incorporates all preceding paragraphs by reference.

143. The California Comprehensive Computer Data Access and Fraud Act ("CCCDAFA") provides for criminal and civil liability against "any person" who, among other specified misconduct, (a) "[k]nowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data"; (b) "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network"; (c) "[k]nowingly and without permission uses or causes to be used computer services"; (d) "[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network"; (e) "[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section"; and (f) "[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network." Cal. Penal Code § 502(c)(1)-(4), (6)-(7). The CCCDAFA provides that, "[i]n addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of" any of these violations "may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief." *Id.* § 502(e)(1).

144. Reynolds's DMS constitutes and is made up of one or more "computer networks," "computer systems," and "computer programs or software," and provides "computer services" to its dealer customers and authorized vendors, including in California, as each of those quoted terms

is defined in the CCCDAFA, Cal. Penal Code § 502(b)(2)-(5). A substantial portion of these networks and systems is located in the State of California, providing computer services to dealer customers located in that State.

145. As set forth above, Authenticom has repeatedly and knowingly accessed the Reynolds DMS without Reynolds's permission, including in California, and has knowingly and without permission engaged in all of the other actions prohibited by the CCCDAFA, Cal. Penal Code § 502(c)(1)-(4), (6)-(7), as quoted above. In particular, Authenticom has knowingly and without permission accessed and used Reynolds's DMS to wrongfully obtain data within the DMS and sell it to third-party vendors; knowingly and without permission attempted to deceive and defraud Reynolds by tricking the DMS into believing that Authenticom was an authorized dealer logging into its own account, when in fact it was not, for the purpose of taking data from the DMS and selling it to third-party vendors; knowingly and without permission used a variety of computer services provided by the Reynolds DMS, without payment for those services; and knowingly and without permission accessing, causing to be accessed, and assisting others in accessing the Reynolds DMS. A substantial portion of these illegal activities either took place in California or were targeted at computers, computer systems, and computer networks located there; were undertaken at the behest of and in coordination with dealers and vendors located in California; and involved confidential data of California residents, including Reynolds's dealer customers located there.

146. Authenticom has caused Reynolds substantial damages and losses by reason of the violations of the CCCDAFA specified above, including the costs of investigating and responding to Authenticom's unlawful actions; the costs of restoring the Reynolds DMS and the data it contains to their condition prior to Authenticom's unlawful actions; and all revenue lost, costs

incurred, and other consequential damages incurred because of disruption of service caused by Authenticom's unauthorized access.

147. Authenticom's violations of the CCCDAFA will continue into the future if not enjoined by this Court. Authenticom's violations have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

148. Furthermore, Reynolds is entitled to equitable relief in the form of restitution for the benefits that it conferred on Authenticom in the form of uncompensated, illegal access to the Reynolds DMS, or disgorgement of the profits that Authenticom earned through its unauthorized and illegal access.

SIXTH COUNTERCLAIM FOR RELIEF
(Tortious Interference With Contract)

149. Reynolds restates and incorporates all preceding paragraphs by reference.

150. Authenticom's own pleadings, motions, evidence, and testimony conclusively establish its liability for tortious interference with Reynolds's contracts with dealers; the only question at this point in the suit is the remedy.

151. Reynolds has binding written contracts with its dealer customers in the form of the Reynolds Customer Agreement.

152. As detailed above, and as admitted by Authenticom, the Reynolds Customer Agreement prohibits customers from allowing third-party integrators like Authenticom to access or use with the DMS without Reynolds's consent. *See supra* ¶¶ 42-51; *Authenticom* Dkt. 1 ¶¶ 150, 152; *Authenticom* Dkt. 63 ¶ 153. These prohibitions in the Reynolds licensing agreements are not in dispute. Authenticom has been aware of these contractual terms for many years because they were common knowledge in the market, and has been aware of the precise contractual language in the Reynolds Customer Agreements since the first quarter of 2015. *Authenticom* Dkt. 162 (6/26/17 Afternoon Session Tr. at 18:17; 19:11-16).

153. Authenticom has long known that, by selling its integration services to Reynolds's customers, instructing them to provide Authenticom with login credentials, and instructing them to allow Authenticom to use its user emulation software and dealer computers to access and use the Reynolds DMS and access and copy information from it, it caused Reynolds's customers to breach their contracts with Reynolds. Nevertheless, Authenticom has acted willfully with the purpose and intent of procuring breaches of the Reynolds Customer Agreements by selling its data bootlegging services to Reynolds's customers. Authenticom's papers are replete with statements confirming that it has actively solicited and induced Reynolds's customers to provide it with login credentials for and access to and use of the Reynolds DMS in violation of the Reynolds Customer Agreements. *E.g.*, *Authenticom* Dkt. 62 at ¶¶ 24-25, 40; *Authenticom* Dkt. 4 at ¶¶ 55, 77-80; *Authenticom* Dkt. 164 (6/26/17 Afternoon Session Tr. at 108:4-7).

154. Authenticom has no justification or privilege that can excuse its tortious interference with Reynolds's dealer contracts. Authenticom's conduct has been willful; its motives have been profit-driven; and it has directly interfered with Reynolds's critical interests in the integrity of its DMS and its relationships with its customers. The court previously rejected

Authenticom's attempt to claim that these DMS contracts violated the antitrust laws, and Authenticom elected not to replead any such claim, thereby conceding that Reynolds's DMS contracts are fully legal and enforceable.

155. Reynolds has been damaged as a direct and proximate result of Authenticom's tortious interference with Reynolds's contracts with its customers. Those damages include but are not limited to damages related to the resulting technical and performance problems for Reynolds's customers that have required Reynolds to devote and divert substantial internal resources for purposes of diagnostic and customer support in response to these technical problems, as well as having to develop additional technological measures to protect the DMS. Moreover, as the direct, proximate, and specifically intended result of Authenticom's tortious interference, it gained valuable, but unauthorized and uncompensated, access to the Reynolds DMS.

156. Authenticom's tortious interference with Reynolds's contracts and business relationships with its customers continues today and will continue into the future if not enjoined by this Court. Authenticom's tortious interference has wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

SEVENTH COUNTERCLAIM FOR RELIEF
(Trespass to Chattels)

157. Reynolds restates and incorporates all preceding paragraphs by reference.

158. Authenticom's continuing efforts to use and intermeddle with Reynolds's DMS over Reynolds's repeated objections and technological blocks constitute trespass to chattels. Authenticom's acts of trespass have not been occasional or accidental, but repeated, intentional, and in willful disregard of Reynolds's objections and demands to cease and desist.

159. The system load and instability caused by Authenticom's repeated and ongoing acts of trespass into Reynolds's DMS have impaired the condition, quality, and value of the DMS; interfered with Reynolds's operation of the DMS and its customers' use and enjoyment of the DMS; and undermined the security and integrity of the DMS and the data stored in it.

160. Authenticom's trespasses have directly and proximately harmed Reynolds by diminishing the functionality, efficiency, and usefulness of its computer systems.

161. Authenticom's trespasses into Reynolds's DMS continue today and will continue into the future if not enjoined by this Court. Authenticom's trespasses have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

EIGHTH COUNTERCLAIM FOR RELIEF
(Conversion)

162. Reynolds restates and incorporates all preceding paragraphs by reference.

163. Every time Authenticom accessed and ran the Reynolds DMS PC software program, it intentionally controlled Reynolds-owned servers, which are located at the dealer sites or at Reynolds's server farms. Use of the DMS PC software program sends instructions to the Reynolds-owned server systems, which execute the instructions and send back a response.

164. As laid out in exhaustive detail in this complaint, Reynolds did not consent to Authenticom's exercise of control over its server systems.

165. Authenticom's relentless onslaught of unauthorized access to the DMS system seriously interfered with Reynolds's possessory rights in its server systems by reducing the efficiency and efficacy of the server systems, thereby crowding out legitimate transactions, and Reynolds has been directly and proximately harmed thereby.

166. Authenticom's conversion of Reynolds's servers for its own use will continue into the future if not enjoined by this court. Authenticom's conversion of Reynolds's servers has wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

NINTH COUNTERCLAIM FOR RELIEF
(Unjust Enrichment)

167. Reynolds restates and incorporates all preceding paragraphs by reference.

168. Liability for "unjust enrichment" exists where one party confers a benefit upon another party; the recipient recognizes and appreciates the fact of such benefit; and the recipient accepts and retains the benefit under circumstances such that it would be inequitable to retain the benefit without payment of the value thereof.

169. As the result of Authenticom's actions described above, Reynolds has involuntarily conferred upon it substantial benefits—access to the Reynolds DMS, usage of the functionalities and data therein, and the ability to "extract" and "scrape" data in the DMS for sale to third parties. Reynolds has invested hundreds of millions of dollars in developing its DMS. Through its unauthorized "pipeline" into the DMS, Authenticom has sought to leech off Reynolds's capital

investments, using and accessing many DMS capabilities free of charge, under no supervision, and without restriction.

170. Authenticom obviously recognizes and appreciates the benefits it has obtained through its unauthorized "pipeline" into the Reynolds DMS and the data in it, as evidenced by its continuing efforts to hack into the DMS despite Reynolds's repeated objections, technological blocks, and threats of litigation.

171. Authenticom has accepted and retained these ill-gotten benefits under circumstances such that it would be inequitable to allow it to retain the benefits without payment of the value thereof in the form of a reasonable licensing and access fee. Authenticom's challenged conduct is illegal under federal and state law; it has brazenly ignored Reynolds's repeated objections and continued with its technological gamesmanship to circumvent Reynolds's security measures, resulting in increased expenses and DMS problems for Reynolds; it has knowingly and intentionally induced Reynolds's dealer customers to breach their license agreements in order to facilitate Authenticom's unauthorized access into the DMS; and it has enjoyed many of the benefits of the DMS without paying anything for access into it. It would be inequitable in these circumstances to allow Authenticom to retain the benefits of its illegal bootlegging business.

172. Authenticom's acts of unjust enrichment at Reynolds's expense continue today and will continue into the future if not enjoined by this Court. Authenticom's actions have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

TENTH COUNTERCLAIM FOR RELIEF
(California Unfair Competition Law)

173. Reynolds restates and incorporates all preceding paragraphs by reference.

174. The California Unfair Competition Law prohibits "any unlawful, unfair or fraudulent business act or practice . . . ." Cal. Bus. & Prof. Code § 17200.

175. Authenticom's business practices, including without limitation misappropriation and unauthorized use of DMS login credentials; copyright infringement; circumvention of access and anticopying controls; and provision to the public of a service that facilitates circumvention of access and anticopying controls; are unlawful for the reasons identified in this complaint. Specifically, Authenticom's conduct violates, without limitation, the federal Computer Fraud and Abuse Act; the Wisconsin Computer Crimes Act; the California Comprehensive Computer Data Access and Fraud Act; the Copyright Act; and the Digital Millennium Copyright Act.

176. A substantial portion of these unlawful activities occurred in California, the largest automobile market in the United States, where huge numbers of Reynolds DMS customers are located.

177. As detailed throughout this complaint, Reynolds has suffered economic injury as a result of Authenticom's unlawful business practices. Authenticom's data-scraping activities have damaged Reynolds's computer systems and forced Reynolds to divert manpower and money to respond to its attacks. Moreover, Authenticom has benefitted from accessing the Reynolds DMS system and the data contained on that system without compensation.

178. Reynolds is entitled to restitution for the uncompensated benefits it has conferred on Authenticom.

179. Authenticom's unlawful business practices will continue into the future if not enjoined by this Court. Authenticom's unlawful business practices have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without

injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

ELEVENTH COUNTERCLAIM FOR RELIEF
(Fraud)

180. Reynolds restates and incorporates all preceding paragraphs by reference.

181. Every time Authenticom logs onto, accesses, and uses the Reynolds DMS, it represents that it is a bona fide, human employee of a Reynolds DMS dealership customer who is authorized to access the DMS. It enters login credentials that are available only to authorized dealership employees and answers—in the affirmative—security questions that inquire whether the user is human.

182. Those representations are false. Authenticom's user emulation software is not human, is not a dealership employee, and it has no authorization to access the DMS.

183. Authenticom knows that it is not a dealership employee, that its automated software scripts are not human, and that it has no authorization to access the DMS.

184. Authenticom presents false login credentials and false security question answers in order to deceive Reynolds into allowing it to access and use the DMS system.

185. Authenticom's deception has been successful during the relevant time period. Reynolds is often unable to determine that Authenticom is not in fact a bona fide, human employee of a Reynolds DMS customer who is authorized to access the DMS, and so Reynolds believes Authenticom's representations and allows Authenticom—masquerading as a dealership employee—to log onto, access, and use the DMS. If Reynolds knew that Authenticom, rather than a bona fide, human employee of a Reynolds DMS dealership customer, was the party attempting to log onto, access, and use the DMS, it would prevent Authenticom from doing so.

186. Reynolds has been damaged as the direct and proximate result of Authenticom's fraud. Those damages include but are not limited to damages related to the technical and performance problems for Reynolds's customers caused by Authenticom's uncontrolled access and the system strain it causes. These problems have required Reynolds to devote and divert substantial internal resources for purposes of diagnostic and customer support in response to these technical problems, as well as having to develop additional technological blocks to protect the DMS. Moreover, as the direct, proximate, and specifically intended result of Authenticom's fraud, it gained valuable, but unauthorized and uncompensated, access to the Reynolds DMS.

187. Authenticom's fraud will continue into the future if not enjoined by this Court. Authenticom's fraud and the uncontrolled, unmonitored, and unauthorized system access it has enabled have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's fraudulent access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

PRAYER FOR RELIEF

WHEREFORE, Reynolds respectfully requests that this Court enter judgment:

A. Declaring that Authenticom's actions:

(1) violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

(2) infringe Reynolds's copyrights in the DMS PC software programs;

(3) violate the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(1)(A), 1201(a)(2), and 1201(b)(1);

(5) violate the Wisconsin Computer Crimes Act, Wis. Stat. § 943.70(2)(a);

(6) violate the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502;

(7) constitute tortious interference with contract, trespass to chattels, conversion, unjust enrichment, and fraud in violation of Wisconsin common law; and

(8) violate the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200;

B. Permanently enjoining Authenticom from engaging in the actions that violate these laws including accessing, using, and copying the Reynolds DMS without Reynolds's authorization (including prohibiting access in violation of Reynolds's unchallenged dealer licensing contracts);

C. Awarding Reynolds its full losses, expenses, and other damages caused by Authenticom's illegal actions;

D. Requiring Authenticom to pay for the benefits it has unjustly obtained through its unauthorized access to Reynolds's DMS and the data in it, including a reasonable royalty together with the profits it has earned from vendors or dealers from accessing the DMS without Reynolds's authorization;

E. Awarding Reynolds its costs and litigation expenses, including attorneys' fees and costs; and

G. Awarding Reynolds such other and further relief that this Court deems just, proper, and equitable.

Dated: June 29, 2018

Respectfully submitted,

/s/ Aundrea K. Gulley
Aundrea K. Gulley
agulley@gibbsbruns.com
Kathy Patrick
kpatrick@gibbsbruns.com
Brian T. Ross
bross@gibbsbruns.com
Brice A. Wilkinson
bwilkinson@gibbsbruns.com
Ross M. MacDonald
rmacdonald@gibbsbruns.com
Justin D. Patrick
jpatrick@gibbsbruns.com
GIBBS & BRUNS, LLP
1100 Louisiana, Suite 5300
Houston, Texas 77002
Telephone: 713-650-8805
Facsimile: 713-750-0903

Michael P.A. Cohen
MCohen@sheppardmullin.com
Amar S. Naik
ANaik@sheppardmullin.com
SHEPPARD MULLIN RICHTER & HAMPTON LLP
Suite 100
2099 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
Telephone: 202-747-1900
Facsimile: 202-747-1901

Leo D. Caseria
SHEPPARD MULLIN RICHTER & HAMPTON, LLP
333 S. Hope St., 43rd Floor
Los Angeles, CA 90071
(213) 617-4206
lcaseria@sheppardmullin.com

Dylan I. Ballard
SHEPPARD MULLIN RICHTER

& HAMPTON, LLP
Four Embarcadero Center., 17th Floor
San Francisco, CA 94111
(415) 434-9100
dballard@sheppardmullin.com

Attorneys for Defendant and Counterplaintiff The Reynolds and Reynolds Company

CERTIFICATE OF SERVICE

I hereby certify that on this 29th day of June, 2018, I caused a true and correct copy of the foregoing Answer, Affirmative Defenses, and Counterclaims to be served on all counsel of record via email.

/s/ Aundrea K. Gulley
Aundrea K. Gulley